BEST AVAILABLE COPY

PCT/JP2004/009608

30. 6. 2004

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

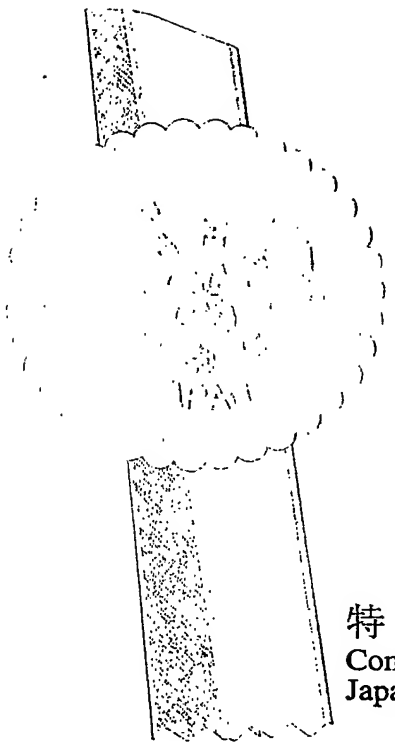
出 願 年 月 日
Date of Application: ２００４年 ６月１７日

出 願 番 号
Application Number: 特願２００４－１７９５６２

[ST. 10/C]: ［ＪＰ２００４－１７９５６２］

出 願 人
Applicant(s): ソニー株式会社

PRIO 19 AUG 2004
WIPO PCT



PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

２００４年 ８月 ６日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号 出証特２００４－３０７０１１０

【書類名】　特許願
【整理番号】　0400036509
【提出日】　平成16年 6月17日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 13/00
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　勝部　友浩
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　伊達　秀樹
【発明者】
　【住所又は居所】　東京都品川区北品川４－７－３５　ソニーグローバルソリューションズ株式会社内
　【氏名】　佐藤　敦司
【発明者】
　【住所又は居所】　東京都品川区北品川４－７－３５　ソニーグローバルソリューションズ株式会社内
　【氏名】　杉田　優
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　三浦　貴之
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　小野　剛
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　宮田　耕自
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
【代理人】
　【識別番号】　100096655
　【弁理士】
　【氏名又は名称】　川井　隆
【選任した代理人】
　【識別番号】　100091225
　【弁理士】
　【氏名又は名称】　仲野　均
【先の出願に基づく優先権主張】
　【出願番号】　特願2003-188139
　【出願日】　平成15年 6月30日
【手数料の表示】
　【予納台帳番号】　087218
　【納付金額】　16,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1

【包括委任状番号】　0114150

【書類名】特許請求の範囲
【請求項１】
提供サーバと端末機器から成り、機器認証サーバで機器認証する際の機器認証情報を端末機器に組み込む機器認証情報組込システムであって、
前記提供サーバは、
機器認証情報を生成する元となる元情報を前記端末機器に提供すると共に、前記機器認証情報、又は前記元情報を、前記端末機器の機器認証を行う機器認証サーバに提供し、
前記端末機器は、
前記提供された元情報を用いて、機器認証情報を送信するために必要な情報を記憶し、機器認証時に、前記記憶した情報を用いて前記元情報から生成した機器認証情報を、前記機器認証サーバに送信する
ことを特徴とする機器認証情報組込システム。
【請求項２】
前記提供サーバは、前記元情報から生成される機器認証情報を所定の一方向性関数で変換した変換値を前記端末機器に提供し、
前記端末機器は、前記提供された元情報から生成した機器認証情報を前記一方向性関数で変換して変換値を生成し、
前記生成した変換値と、前記提供サーバから提供された変換値の同一性を判断することを特徴とする請求項１に記載の機器認証情報組込システム。
【請求項３】
前記端末機器は、前記提供された元情報から生成した機器認証情報を所定の一方向性関数で変換して変換値を前記提供サーバに提供し、
前記提供サーバは、前記元情報から生成される機器認証情報を前記一方向性関数で変換した変換値と、前記端末機器から提供された変換値の同一性を判断することを特徴とする請求項１に記載の機器認証情報組込システム。
【請求項４】
提供サーバから提供される、機器認証情報を生成する元となる元情報を取得する元情報取得手段と、
前記取得した元情報から機器認証情報を生成する生成手段と、
機器認証時に、前記生成した機器認証情報を機器認証サーバに送信する機器認証情報送信手段と、
を具備したことを特徴とする端末機器。
【請求項５】
前記元情報は、前記機器認証情報を暗号化した暗号化機器認証情報であり、
前記生成手段は、前記暗号化機器認証情報を復号化することにより、前記機器認証情報を生成することを特徴とする請求項４に記載の端末機器。
【請求項６】
前記生成手段で生成した機器認証情報を暗号化して記憶する記憶手段を具備し、
前記機器認証情報送信手段は、前記記憶手段に記憶された機器認証情報を復号化して送信することを特徴とする請求項４に記載の端末機器。
【請求項７】
前記記憶手段に記憶する機器認証情報の暗号化、及び復号化に使用する暗号鍵を、前記暗号鍵の使用時に前記端末機器に固有な情報を用いて生成する鍵生成手段を具備したことを特徴とする請求項６に記載の端末機器。
【請求項８】
前記生成した暗号鍵を、前記暗号鍵の使用後の所定期間内に消去する鍵消去手段を具備したことを特徴とする請求項７に記載の端末機器。
【請求項９】
前記提供サーバから前記機器認証情報を所定の一方向性関数で変換した変換値を取得する変換値取得手段と、

前記生成した機器認証情報を、前記一方向性関数で変換して変換値を算出する変換値算出手段と、
前記取得した変換値と、前記算出した変換値の同一性を判断し、その判断結果を出力する判断手段と、
を具備したことを特徴とする請求項４に記載の端末機器。
【請求項１０】
前記生成した機器認証情報を他の一方向性関数で変換して変換値を算出する変換値算出手段と、
前記算出した変換値を前記提供サーバに提供する変換値提供手段と、
を具備したことを特徴とする請求項９に記載の端末機器。
【請求項１１】
前記生成した機器認証情報を所定の一方向性関数で変換して変換値を算出する変換値算出手段と、
前記算出した変換値を前記提供サーバに提供する変換値提供手段と、
を具備したことを特徴とする請求項４に記載の端末機器。
【請求項１２】
前記取得した元情報を記憶する記憶手段を具備し、
前記機器認証情報送信手段は、前記記憶した元情報から機器認証情報を生成して前記機器認証サーバに送信することを特徴とする請求項４に記載の端末機器。
【請求項１３】
元情報取得手段と、生成手段と、機器認証情報送信手段と、を備えたコンピュータで構成された端末機器において、
提供サーバから提供される、機器認証情報を生成する元となる元情報を前記元情報取得手段で取得する元情報取得ステップと、
前記取得した元情報から機器認証情報を、前記生成手段で生成する生成ステップと、
機器認証時に、前記生成した機器認証情報を、前記機器認証情報送信手段で機器認証サーバに送信する機器認証情報送信ステップと、
から構成されたことを特徴とする機器認証情報処理方法。
【請求項１４】
前記元情報は、前記機器認証情報を暗号化した暗号化機器認証情報であり、
前記生成ステップでは、前記暗号化機器認証情報を復号化することにより、前記機器認証情報を生成することを特徴とする請求項１３に記載の機器認証情報処理方法。
【請求項１５】
前記コンピュータは、記憶手段を備え、
前記生成手段で生成した機器認証情報を暗号化して前記記憶手段で記憶する記憶ステップを備え、
前記機器認証情報送信ステップでは、前記記憶手段に記憶された機器認証情報を復号化して送信することを特徴とする請求項１３に記載の機器認証情報処理方法。
【請求項１６】
前記コンピュータは、鍵生成手段を備え、
前記記憶手段に記憶する機器認証情報の暗号化、及び復号化に使用する暗号鍵を、前記鍵生成手段で前記暗号鍵の使用時に前記端末機器に固有な情報を用いて生成する鍵生成ステップを備えたことを特徴とする請求項１５に記載の機器認証情報処理方法。
【請求項１７】
前記コンピュータは、鍵消去手段を備え、
前記生成した暗号鍵を、前記暗号鍵の使用後の所定期間内に前記鍵消去手段で消去する鍵消去ステップを備えたことを特徴とする請求項１６に記載の機器認証情報処理方法。
【請求項１８】
前記コンピュータは、変換値取得手段と、変換値算出手段と、判断手段と、を備え、
前記提供サーバから前記機器認証情報を所定の一方向性関数で変換した変換値を前記変

換値取得手段で取得する変換値取得ステップと、
　前記変換値算出手段で前記生成した機器認証情報を、前記一方向性関数で変換して変換値を算出する変換値算出ステップと、
　前記判断手段で、前記取得した変換値と、前記算出した変換値の同一性を判断し、その判断結果を出力する判断ステップと、
　を備えたことを特徴とする請求項１３に記載の機器認証情報処理方法。
【請求項１９】
　前記コンピュータは、変換値算出手段と、変換値提供手段と、を備え、
　前記変換値算出手段で、前記生成した機器認証情報を他の一方向性関数で変換して変換値を算出する変換値算出ステップと、
　前記変換値算出手段で、前記算出した変換値を前記提供サーバに提供する変換値提供ステップと、
　を備えたことを特徴とする請求項１８に記載の機器認証情報処理方法。
【請求項２０】
　前記コンピュータは、変換値算出手段と、変換値提供手段と、を備え、
　前記変換値算出手段で、前記生成した機器認証情報を所定の一方向性関数で変換して変換値を算出する変換値算出ステップと、
　前記変換値提供手段で、前記算出した変換値を前記提供サーバに提供する変換値提供ステップと、
　を備えたことを特徴とする請求項１３に記載の機器認証情報処理方法。
【請求項２１】
　前記コンピュータは、前記取得した元情報を記憶する記憶手段を具備し、
　前記機器認証情報送信ステップでは、前記記憶した元情報から機器認証情報を生成して前記機器認証サーバに送信することを特徴とする請求項１３に記載の機器認証情報処理方法。
【請求項２２】
　提供サーバから提供される、機器認証情報を生成する元となる元情報を取得する元情報取得機能と、
　前記取得した元情報から機器認証情報を生成する生成機能と、
　機器認証時に、前記生成した機器認証情報を機器認証サーバに送信する機器認証情報送信機能と、
　をコンピュータで実現する機器認証情報処理プログラム。
【請求項２３】
　前記元情報は、前記機器認証情報を暗号化した暗号化機器認証情報であり、
　前記生成機能は、前記暗号化機器認証情報を復号化することにより、前記機器認証情報を生成することを特徴とする請求項２２に記載の機器認証情報処理プログラム。
【請求項２４】
　前記生成機能で生成した機器認証情報を暗号化して記憶する記憶機能を実現し、
　前記機器認証情報送信機能は、前記記憶機能に記憶された機器認証情報を復号化して送信することを特徴とする請求項２２に記載の機器認証情報処理プログラム。
【請求項２５】
　前記記憶機能に記憶する機器認証情報の暗号化、及び復号化に使用する暗号鍵を、前記暗号鍵の使用時に前記端末機器に固有な情報を用いて生成する鍵生成機能をコンピュータで実現する請求項２４に記載の機器認証情報処理プログラム。
【請求項２６】
　前記生成した暗号鍵を、前記暗号鍵の使用後の所定期間内に消去する鍵消去機能をコンピュータで実現する請求項２５に記載の機器認証情報処理プログラム。
【請求項２７】
　前記提供サーバから前記機器認証情報を所定の一方向性関数で変換した変換値を取得する変換値取得機能と、

前記生成した機器認証情報を、前記一方向性関数で変換して変換値を算出する変換値算出機能と、
前記取得した変換値と、前記算出した変換値の同一性を判断し、その判断結果を出力する判断機能と、
をコンピュータで実現する請求項２２に記載の機器認証情報処理プログラム。
【請求項２８】
前記生成した機器認証情報を他の一方向性関数で変換して変換値を算出する変換値算出機能と、
前記算出した変換値を前記提供サーバに提供する変換値提供機能と、
をコンピュータで実現する請求項２７に記載の機器認証情報処理プログラム。
【請求項２９】
前記生成した機器認証情報を所定の一方向性関数で変換して変換値を算出する変換値算出機能と、
前記算出した変換値を前記提供サーバに提供する変換値提供機能と、
をコンピュータで実現する請求項２２に記載の機器認証情報処理プログラム。
【請求項３０】
前記取得した元情報を記憶する記憶機能をコンピュータで実現し、
前記機器認証情報送信機能は、前記記憶した元情報から機器認証情報を生成して前記機器認証サーバに送信することを特徴とする請求項２２に記載の機器認証情報処理プログラム。
【請求項３１】
提供サーバから提供される、機器認証情報を生成する元となる元情報を取得する元情報取得機能と、
前記取得した元情報から機器認証情報を生成する生成機能と、
機器認証時に、前記生成した機器認証情報を機器認証サーバに送信する機器認証情報送信機能と、
をコンピュータで実現する機器認証情報処理プログラムを記憶したコンピュータが読み取り可能な記憶媒体。
【請求項３２】
端末機器に機器認証情報を生成する元となる元情報を提供する元情報提供手段と、
前記機器認証情報、又は前記元情報を、前記端末機器の機器認証を行う機器認証サーバに提供する機器認証情報提供手段と、
前記端末機器から、前記元情報から生成された機器認証情報の、所定の一方向性関数で変換した変換値を取得する変換値取得手段と、
前記機器認証情報を前記一方向性関数で変換して変換値を算出する変換値算出手段と、
前記取得した変換値と前記算出した変換値の同一性を判断し、その判断結果を出力する判断手段と、
を具備したことを特徴とする提供サーバ。
【請求項３３】
前記判断手段で出力された判断結果を、前記元情報の組込主体に送信する判断結果送信手段を具備したことを特徴とする請求項３２に記載の提供サーバ。
【請求項３４】
元情報提供手段と、機器認証情報提供手段と、変換値取得手段と、変換値算出手段と、判断手段と、を備えたコンピュータにおいて、
端末機器に機器認証情報を生成する元となる元情報を、前記元情報提供手段で提供する元情報提供ステップと、
前記機器認証情報、又は前記元情報を、前記機器認証情報提供手段で前記端末機器の機器認証を行う機器認証サーバに提供する機器認証情報提供ステップと、　前記変換値取得手段で、前記端末機器から、前記元情報から生成された機器認証情報の、所定の一方向性関数で変換した変換値を取得する変換値取得ステップと、

前記変換値算出手段で、前記機器認証情報を前記一方向性関数で変換して変換値を算出する変換値算出ステップと、
前記判断手段で、前記取得した変換値と前記算出した変換値の同一性を判断し、その判断結果を出力する判断ステップと、
から構成されたことを特徴とする機器認証情報提供方法。
【請求項３５】
前記コンピュータは、判断結果送信手段を備え、
前記判断手段で出力された判断結果を、前記判断結果送信手段で前記元情報の組込主体に送信する判断結果送信ステップを備えたことを特徴とする請求項３４に記載の機器認証情報提供方法。
【請求項３６】
端末機器に機器認証情報を生成する元となる元情報を提供する元情報提供機能と、
前記機器認証情報、又は前記元情報を、前記端末機器の機器認証を行う機器認証サーバに提供する機器認証情報提供機能と、
前記端末機器から、前記元情報から生成された機器認証情報の、所定の一方向性関数で変換した変換値を取得する変換値取得機能と、
前記機器認証情報を前記一方向性関数で変換して変換値を算出する変換値算出機能と、
前記取得した変換値と前記算出した変換値の同一性を判断し、その判断結果を出力する判断機能と、
をコンピュータで実現する機器認証情報提供プログラム。
【請求項３７】
前記判断機能で出力された判断結果を、前記元情報の組込主体に送信する判断結果送信機能をコンピュータで実現する請求項３６に記載の機器認証情報提供プログラム。
【請求項３８】
端末機器に機器認証情報を生成する元となる元情報を提供する元情報提供機能と、
前記機器認証情報、又は前記元情報を、前記端末機器の機器認証を行う機器認証サーバに提供する機器認証情報提供機能と、
前記端末機器から、前記元情報から生成された機器認証情報の、所定の一方向性関数で変換した変換値を取得する変換値取得機能と、
前記機器認証情報を前記一方向性関数で変換して変換値を算出する変換値算出機能と、
前記取得した変換値と前記算出した変換値の同一性を判断し、その判断結果を出力する判断機能と、
をコンピュータで実現する機器認証情報提供プログラムを記憶したコンピュータが読み取り可能な記憶媒体。

【書類名】明細書
【発明の名称】機器認証情報組込システム、端末機器、機器認証情報処理方法、機器認証情報処理プログラム、提供サーバ、機器認証情報提供方法、機器認証情報提供プログラム、及び記憶媒体
【技術分野】
【０００１】
本発明は、端末機器などに関し、特に、機器認証情報を暗号化して機器に書き込み、これを機器内で復号化することにより、機器認証情報を安全に機器内に書き込むものに関する。
【背景技術】
【０００２】
近年、ＣＥ（ＣＥ：Ｃｏｎｓｕｍｅｒ　Ｅｌｅｃｔｒｏｎｉｃｓ）機器の普及が広まりつつある。ＣＥ機器とは、例えば、ビデオデッキ、ステレオ、テレビなどのオーディオビジュアル機器や、炊飯器、冷蔵庫などの家電製品や、その他の電子機器にコンピュータを内蔵させ、ネットワークを介してサービスを利用できるものである。
サーバが提供するサービスには、ＣＥ機器の機器認証を要するものがある。そのため、ＣＥ機器には、機器認証を行うための機器認証情報が予め製造工場にて組み込まれる。
【０００３】
図１８は、従来の機器認証情報の組み込み方法を説明するための図である。ＣＥ機器に組み込まれる機器認証情報は、管理センタ１０３の管理サーバ１０７で管理されている。
管理サーバ１０７は、機器認証情報をＣＥ機器の製造工場である工場１０５に送信する。
機器認証情報は、機密性を要する秘密情報であるので、外部に漏出しないように暗号化されて送信される。
【０００４】
工場１０５では、接続手段１１０をＣＥ機器１０９のコネクタに接続して、管理サーバ１０７から送信されてきた機器認証情報をＣＥ機器１０９に入力する。　接続手段１１０には、暗号化された機器認証情報を復号化する機能が内蔵されており、管理サーバ１０７から送信されてきた機器認証情報は、接続手段１１０にて復号化される。
機器認証情報は、復号化された状態で接続手段１１０からＣＥ機器１０９に入力されて、ＣＥ機器１０９の記憶装置に記憶される。
このような、ＣＥ機器に機器認証情報を組み込む発明としては、次の電子機器製造システム及び電子機器製造方法がある。
【０００５】
【特許文献１】特開２００１－１３４６５４
【０００６】
この発明は、ＣＥ機器に貼付したバーコードラベルシールに書かれた製品シリアル番号から、データベースに登録されている機器認証情報を読み出して機器に組み込むものである。
【発明の開示】
【発明が解決しようとする課題】
【０００７】
ところが、従来の方法では、接続手段１１０で機器認証情報を復号化してしまうため、接続手段１１０から機器認証情報が漏出してしまう可能性があった。
特に近年では、コストの低い海外の事業者に生産を委託する場合なども多く、工場１０５に送った機器認証情報が外部に漏出することなく確実にＣＥ機器１０９に組み込める仕組みが必要とされていた。
【０００８】
そこで、本発明の第１の目的は、機器内に機器認証情報を安全に組み込むことができる端末機器などを提供することである。

また、本発明の第２の目的は、機器内に機器認証情報が適切に組み込まれたことを機器認証情報の秘密状態を保持した状態で確認することである。

【課題を解決するための手段】

【０００９】

本発明は、前記目的を達成するために、提供サーバと端末機器から成り、機器認証サーバで機器認証する際の機器認証情報を端末機器に組み込む機器認証情報組込システムであって、前記提供サーバは、機器認証情報を生成する元となる元情報を前記端末機器に提供すると共に、前記機器認証情報、又は前記元情報を、前記端末機器の機器認証を行う機器認証サーバに提供し、前記端末機器は、前記提供された元情報を用いて、機器認証情報を送信するために必要な情報を記憶し、機器認証時に、前記記憶した情報を用いて前記元情報から生成した機器認証情報を、前記機器認証サーバに送信することを特徴とする機器認証情報組込システムを提供する（第１の構成）。

第１の構成において、前記提供サーバは、前記元情報から生成される機器認証情報を所定の一方向性関数で変換した変換値を前記端末機器に提供し、前記端末機器は、前記提供された元情報から生成した機器認証情報を前記一方向性関数で変換して変換値を生成し、前記生成した変換値と、前記提供サーバから提供された変換値の同一性を判断するように構成することができる（第２の構成）。

また、第１の構成において、前記端末機器は、前記提供された元情報から生成した機器認証情報を所定の一方向性関数で変換して変換値を前記提供サーバに提供し、前記提供サーバは、前記元情報から生成される機器認証情報を前記一方向性関数で変換した変換値と、前記端末機器から提供された変換値の同一性を判断するように構成することもできる（第３の構成）。

また、本発明は、前記目的を達成するために、提供サーバから提供される、機器認証情報を生成する元となる元情報を取得する元情報取得手段と、前記取得した元情報から機器認証情報を生成する生成手段と、機器認証時に、前記生成した機器認証情報を機器認証サーバに送信する機器認証情報送信手段と、を具備したことを特徴とする端末機器を提供する（第４の構成）。

また、第４の構成において、前記元情報は、前記機器認証情報を暗号化した暗号化機器認証情報であり、前記生成手段は、前記暗号化機器認証情報を復号化することにより、前記機器認証情報を生成するように構成することもできる（第５の構成）。

更に、第４の構成において、前記生成手段で生成した機器認証情報を暗号化して記憶する記憶手段を具備し、前記機器認証情報送信手段は、前記記憶手段に記憶された機器認証情報を復号化して送信するように構成することもできる（第６の構成）。

また、第６の構成において、前記記憶手段に記憶する機器認証情報の暗号化、及び復号化に使用する暗号鍵を、前記暗号鍵の使用時に前記端末機器に固有な情報を用いて生成する鍵生成手段を具備するように構成することもできる（第７の構成）。

また、第７の構成において、前記生成した暗号鍵を、前記暗号鍵の使用後の所定期間内に消去する鍵消去手段を具備するように構成することもできる（第８の構成）。

また、第４の構成において、前記提供サーバから前記機器認証情報を所定の一方向性関数で変換した変換値を取得する変換値取得手段と、前記生成した機器認証情報を、前記一方向性関数で変換して変換値を算出する変換値算出手段と、前記取得した変換値と、前記算出した変換値の同一性を判断し、その判断結果を出力する判断手段と、を具備するように構成することもできる（第９の構成）。

また、第９の構成において、前記生成した機器認証情報を他の一方向性関数で変換して変換値を算出する変換値算出手段と、前記算出した変換値を前記提供サーバに提供する変換値提供手段と、を具備するように構成することもできる（第１０の構成）。

また、第４の構成において、前記生成した機器認証情報を所定の一方向性関数で変換して変換値を算出する変換値算出手段と、前記算出した変換値を前記提供サーバに提供する変換値提供手段と、を具備するように構成することもできる（第１１の構成）。

また、第４の構成において、前記取得した元情報を記憶する記憶手段を具備し、前記機

器認証情報送信手段は、前記記憶した元情報から機器認証情報を生成して前記機器認証サーバに送信するように構成することもできる（第１２の構成）。

また、本発明は、前記目的を達成するために、元情報取得手段と、生成手段と、機器認証情報送信手段と、を備えたコンピュータで構成された端末機器において、提供サーバから提供される、機器認証情報を生成する元となる元情報を前記元情報取得手段で取得する元情報取得ステップと、前記取得した元情報から機器認証情報を、前記生成手段で生成する生成ステップと、機器認証時に、前記生成した機器認証情報を、前記機器認証情報送信手段で機器認証サーバに送信する機器認証情報送信ステップと、から構成されたことを特徴とする機器認証情報処理方法を提供する（第１３の構成）。

また、第１３の構成において、前記元情報は、前記機器認証情報を暗号化した暗号化機器認証情報であり、前記生成ステップでは、前記暗号化機器認証情報を復号化することにより、前記機器認証情報を生成するように構成することもできる（第１４の構成）。

また、第１３の構成において、前記コンピュータは、記憶手段を備え、前記生成手段で生成した機器認証情報を暗号化して前記記憶手段で記憶する記憶ステップを備え、前記機器認証情報送信ステップでは、前記記憶手段に記憶された機器認証情報を復号化して送信するように構成することもできる（第１５の構成）。

また、第１５の構成において、前記コンピュータは、鍵生成手段を備え、前記記憶手段に記憶する機器認証情報の暗号化、及び復号化に使用する暗号鍵を、前記鍵生成手段で前記暗号鍵の使用時に前記端末機器に固有な情報を用いて生成する鍵生成ステップを備えるように構成することもできる（第１６の構成）。

また、第１６の構成において、前記コンピュータは、鍵消去手段を備え、前記生成した暗号鍵を、前記暗号鍵の使用後の所定期間内に前記鍵消去手段で消去する鍵消去ステップを備えるように構成することもできる（第１７の構成）。

また、第１３の構成において、前記コンピュータは、変換値取得手段と、変換値算出手段と、判断手段と、を備え、前記提供サーバから前記機器認証情報を所定の一方向性関数で変換した変換値を前記変換値取得手段で取得する変換値取得ステップと、前記変換値算出手段で前記生成した機器認証情報を、前記一方向性関数で変換して変換値を算出する変換値算出ステップと、前記判断手段で、前記取得した変換値と、前記算出した変換値の同一性を判断し、その判断結果を出力する判断ステップと、を備えるように構成することもできる（第１８の構成）。

また、第１８の構成において、前記コンピュータは、変換値算出手段と、変換値提供手段と、を備え、前記変換値算出手段で、前記生成した機器認証情報を他の一方向性関数で変換して変換値を算出する変換値算出ステップと、前記変換値算出手段で、前記算出した変換値を前記提供サーバに提供する変換値提供ステップと、を備えるように構成することができる（第１９の構成）。

第１３の構成において、前記コンピュータは、変換値算出手段と、変換値提供手段と、を備え、前記変換値算出手段で、前記生成した機器認証情報を所定の一方向性関数で変換して変換値を算出する変換値算出ステップと、前記変換値提供手段で、前記算出した変換値を前記提供サーバに提供する変換値提供ステップと、を備えるように構成することができる（第２０の構成）。

また、第１３の構成において、前記コンピュータは、前記取得した元情報を記憶する記憶手段を具備し、前記機器認証情報送信ステップでは、前記記憶した元情報から機器認証情報を生成して前記機器認証サーバに送信するように構成することができる（第２１の構成）。

また、本発明は、前記目的を達成するために、提供サーバから提供される、機器認証情報を生成する元となる元情報を取得する元情報取得機能と、前記取得した元情報から機器認証情報を生成する生成機能と、機器認証時に、前記生成した機器認証情報を機器認証サーバに送信する機器認証情報送信機能と、をコンピュータで実現する機器認証情報処理プログラムを提供する（第２２の構成）。

第２２の構成において、前記元情報は、前記機器認証情報を暗号化した暗号化機器認証

情報であり、前記生成機能は、前記暗号化機器認証情報を復号化することにより、前記機器認証情報を生成するように構成することができる（第２３の構成）。

第２２の構成において、前記生成機能で生成した機器認証情報を暗号化して記憶する記憶機能を実現し、前記機器認証情報送信機能は、前記記憶機能に記憶された機器認証情報を復号化して送信するように構成することができる（第２４の構成）。

第２４の構成において、前記記憶機能に記憶する機器認証情報の暗号化、及び復号化に使用する暗号鍵を、前記暗号鍵の使用時に前記端末機器に固有な情報を用いて生成する鍵生成機能をコンピュータで実現するように構成することもできる（第２５の構成）。

また、第２５の構成において、前記生成した暗号鍵を、前記暗号鍵の使用後の所定期間内に消去する鍵消去機能をコンピュータで実現するように構成することもできる（第２６の構成）。

第２２の構成において、前記提供サーバから前記機器認証情報を所定の一方向性関数で変換した変換値を取得する変換値取得機能と、前記生成した機器認証情報を、前記一方向性関数で変換して変換値を算出する変換値算出機能と、前記取得した変換値と、前記算出した変換値の同一性を判断し、その判断結果を出力する判断機能と、をコンピュータで実現するように構成することができる（第２７の構成）。

第２７の構成において、前記生成した機器認証情報を他の一方向性関数で変換して変換値を算出する変換値算出機能と、前記算出した変換値を前記提供サーバに提供する変換値提供機能と、をコンピュータで実現するように構成することができる（第２８の構成）。

第２２の構成において、前記生成した機器認証情報を所定の一方向性関数で変換して変換値を算出する変換値算出機能と、前記算出した変換値を前記提供サーバに提供する変換値提供機能と、をコンピュータで実現するように構成することができる（第２９の構成）。

第２２の構成において、前記取得した元情報を記憶する記憶機能をコンピュータで実現し、前記機器認証情報送信機能は、前記記憶した元情報から機器認証情報を生成して前記機器認証サーバに送信するように構成することができる（第３０の構成）。

また、本発明は、前記目的を達成するために、提供サーバから提供される、機器認証情報を生成する元となる元情報を取得する元情報取得機能と、前記取得した元情報から機器認証情報を生成する生成機能と、機器認証時に、前記生成した機器認証情報を機器認証サーバに送信する機器認証情報送信機能と、をコンピュータで実現する機器認証情報処理プログラムを記憶したコンピュータが読み取り可能な記憶媒体を提供する（第３１の構成）。

また、本発明は、前記目的を達成するために、端末機器に機器認証情報を生成する元となる元情報を提供する元情報提供手段と、前記機器認証情報、又は前記元情報を、前記端末機器の機器認証を行う機器認証サーバに提供する機器認証情報提供手段と、前記端末機器から、前記元情報から生成された機器認証情報の、所定の一方向性関数で変換した変換値を取得する変換値取得手段と、前記機器認証情報を前記一方向性関数で変換して変換値を算出する変換値算出手段と、前記取得した変換値と前記算出した変換値の同一性を判断し、その判断結果を出力する判断手段と、を具備したことを特徴とする提供サーバを提供する（第３２の構成）。

第３２の構成において、前記判断手段で出力された判断結果を、前記元情報の組込主体に送信する判断結果送信手段を具備するように構成することができる（第３３の構成）。

また、本発明は、前記目的を達成するために、元情報提供手段と、機器認証情報提供手段と、変換値取得手段と、変換値算出手段と、判断手段と、を備えたコンピュータにおいて、端末機器に機器認証情報を生成する元となる元情報を、前記元情報提供手段で提供する元情報提供ステップと、前記機器認証情報、又は前記元情報を、前記機器認証情報提供手段で前記端末機器の機器認証を行う機器認証サーバに提供する機器認証情報提供ステップと、前記変換値取得手段で、前記端末機器から、前記元情報から生成された機器認証情報の、所定の一方向性関数で変換した変換値を取得する変換値取得ステップと、前記変換値算出手段で、前記機器認証情報を前記一方向性関数で変換して変換値を算出する変換値

算出ステップと、前記判断手段で、前記取得した変換値と前記算出した変換値の同一性を判断し、その判断結果を出力する判断ステップと、から構成されたことを特徴とする機器認証情報提供方法を提供する（第３４の構成）。

第３４の構成において、前記コンピュータは、判断結果送信手段を備え、前記判断手段で出力された判断結果を、前記判断結果送信手段で前記元情報の組込主体に送信する判断結果送信ステップを備えるように構成することができる（第３５の構成）。

また、本発明は、前記目的を達成するために、端末機器に機器認証情報を生成する元となる元情報を提供する元情報提供機能と、前記機器認証情報、又は前記元情報を、前記端末機器の機器認証を行う機器認証サーバに提供する機器認証情報提供機能と、前記端末機器から、前記元情報から生成された機器認証情報の、所定の一方向性関数で変換した変換値を取得する変換値取得機能と、前記機器認証情報を前記一方向性関数で変換して変換値を算出する変換値算出機能と、前記取得した変換値と前記算出した変換値の同一性を判断し、その判断結果を出力する判断機能と、をコンピュータで実現する機器認証情報提供プログラムを提供する（第３６の構成）。

第３６の構成において、前記判断機能で出力された判断結果を、前記元情報の組込主体に送信する判断結果送信機能をコンピュータで実現するように構成することができる（第３７の構成）。

また、本発明は、前記目的を達成するために、端末機器に機器認証情報を生成する元となる元情報を提供する元情報提供機能と、前記機器認証情報、又は前記元情報を、前記端末機器の機器認証を行う機器認証サーバに提供する機器認証情報提供機能と、前記端末機器から、前記元情報から生成された機器認証情報の、所定の一方向性関数で変換した変換値を取得する変換値取得機能と、前記機器認証情報を前記一方向性関数で変換して変換値を算出する変換値算出機能と、前記取得した変換値と前記算出した変換値の同一性を判断し、その判断結果を出力する判断機能と、をコンピュータで実現する機器認証情報提供プログラムを記憶したコンピュータが読み取り可能な記憶媒体を提供する（第３８の構成）。

【発明の効果】

【００１０】

本発明によれば、機器内に機器認証情報を安全に組み込むことができる。また、機器内に機器認証情報が適切に組み込まれたことを機器認証情報の秘密状態を保持したまま確認することができる。

【発明を実施するための最良の形態】

【００１１】

以下、本発明の好適な実施の形態について、図を参照して詳細に説明する。

［第１の実施の形態の概要］

図１は、第１の実施の形態の概要を説明するための図である。

機器認証情報を管理する管理サーバ７は、管理センタ３に設置されており、機器認証情報を暗号化して工場５に送信する。

接続手段１０は、工場の作業者によりＣＥ機器９のコネクタに接続され、管理サーバ７から送信されてきた機器認証情報を暗号化されたままの状態でＣＥ機器９に入力する。

ＣＥ機器９の内部には、暗号化された機器認証情報を復号化して格納するための書込モジュールが内蔵されている。

接続手段１０から入力された機器認証情報は、書込モジュールにより復号化され、ＣＥ機器９内部の記憶装置に記憶される。

接続手段１０は、従来例で使用している接続手段１１０とは異なり、管理サーバ７から送信されてきた機器認証情報を復号化せずにＣＥ機器９に入力する。

【００１２】

このように、本実施の形態では、管理サーバ７（提供サーバ）から送信されてきた機器認証情報が暗号化されたままＣＥ機器９（端末機器）に入力されてＣＥ機器９内部で復号化されるので、機器認証情報組み込み作業におけるセキュリティを高めることができる。

なお、以上の説明は、本実施の形態の基本的な概念を説明するためのものであり、各種の変形が可能である。

例えば、以下の実施の形態の詳細で説明するように、復号化した機器認証情報を他の暗号鍵で再度暗号化して記憶装置に記憶することにより、よりセキュリティを高めることができる。

また、本実施の形態では、ＣＥ機器９に機器認証情報が適切に組み込まれたことを工場５、及び管理センタ３が確認する手段も提供する。

【００１３】

［第１の実施の形態の詳細］

図２は、ＣＥ機器の製造認証システム１の構成の一例を示した図である。製造認証システム１は、ＣＥ機器９の製造と機器認証を行うシステムであり、ＣＥ機器９にサービスを提供するサービスサーバなどは図示していない。

製造認証システム１は、事業体１１、管理センタ３、工場５、ＣＥ機器９、機器認証サーバ８などから構成されている。

事業体１１は、ＣＥ機器９の製造会社であり、ＣＥ機器９の企画、開発、販売など、ＣＥ機器９を市場に供給する事業体である。

管理センタ３は、ＣＥ機器９に組み込む機器認証情報の管理を行う部門であり、機器認証情報の発行や、機器認証情報に関する暗号情報を管理している。

【００１４】

工場５は、事業体１１からの依頼により、ＣＥ機器９の製造を行う部門である。工場５は、事業体１１が有する場合もあるし、また、事業体１１の委託を受けてＣＥ機器９を製造する第三者が運営する工場である場合もある。

ＣＥ機器９は、工場５で製造されたＣＥ機器であり、内部に管理センタ３が発行した機器認証情報が組み込まれている。

機器認証サーバ８は、管理センタ３から機器認証情報の提供を受けると共に、ＣＥ機器９から機器認証情報を受信してＣＥ機器９を機器認証するサーバ装置である。

ＣＥ機器９は、機器認証サーバ８で機器認証されることにより、サービスサーバなどが提供するサービスを受けることができる。

【００１５】

以下、製造認証システム１でＣＥ機器９が製造されるプロセスを図中の番号を参照しながら説明する。

（１）まず、事業体１１が、ＣＥ機器９の企画設計を行う。そして、管理センタ３から、ＣＥ機器９にインストールするファームウェアを作成するための情報を取得する。

このファームウェアは、機器認証情報を組み込むためのプログラムやＣＥ機器９を動作させるためのプログラムなどから成り、工場５でＣＥ機器９にインストールされる。事業体１１は、管理センタ３からは、暗号鍵などの機器認証情報を組み込むための情報を取得する。

【００１６】

（２）事業体１１は、ＣＥ機器９の製造を工場５に依頼すると共に、ＣＥ機器９にインストールするファームウェアをＣＤ－ＲＯＭ（Ｃｏｍｐａｃｔ　Ｄｉｓｃ－Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）に記録して送付したり、あるいは、ネットワークを介して送信するなどして工場５に渡す。

（３）工場５は、ＣＥ機器９を組み立てた後、事業体１１から取得したファームウェアをＣＥ機器９にインストールする。そして、ＣＥ機器９のコネクタに接続手段１０（図１）を接続し、管理センタ３に対して機器認証情報の送信を要求する。

【００１７】

（４）管理センタ３は、工場５からの要求に応じてＣＥ機器９に組み込むための機器認証情報をネットワークを介して工場５に送信する。この機器認証情報は、暗号化されている。

この暗号化された機器認証情報は、復号化すると機器認証情報が得られるので、機器認

証情報を生成するための元情報に該当する。機器認証情報の内容については後に詳細に説明する。

（５）工場５は、管理センタ３から送信されてきた機器認証情報を接続手段１０を介してＣＥ機器９に入力する。機器認証情報は、ＣＥ機器９のファームウェアが提供する暗号鍵によりＣＥ機器９内で復号化された後、ファームウェアが提供する他の暗号鍵により再び暗号化されて記憶装置に記憶される。

（６）そして、後述する方法により、ＣＥ機器９に機器認証情報が正しく組み込まれたか否かを、工場５と管理センタ３が確認する。これを用いて、工場５が管理センタ３に製造実績報告を行うことができる。

【００１８】

（７）工場５は、ＣＥ機器９の組み立て、及び機器認証情報の組み込みを完了した後、ＣＥ機器９を出荷する。

（８）管理センタ３は、ＣＥ機器９の機器認証情報を機器認証サーバ８に提供する。

（９）機器認証サーバ８は、ＣＥ機器９から機器認証情報を送信してもらい、これを管理センタ３から提供された機器認証情報と比較することによりＣＥ機器９を機器認証する。

【００１９】

図３は、機器認証部９９の一例を示した図である。機器認証部９９は、工場５でファームウェアをインストールすることにより、ＣＥ機器９の内部で構成された機能部である。

機器認証部９９は、認証モジュール２０、書込モジュール３０、認証情報メモリ４０、本体識別情報メモリ５０などから構成されている。

【００２０】

認証モジュール２０は、ＣＥ機器９を機器認証サーバ８で機器認証するための機能部である。

認証モジュール２０は、機器認証サーバ８に認証情報を送信する際に使用する公開鍵２１、固有鍵２３を生成するための固有鍵生成子２２を備えている。

【００２１】

固有鍵２３は、認証情報メモリ４０に記憶する機器認証情報を暗号化、及び復号化するための鍵情報であり、使用時に固有鍵生成子２２とＭＡＣアドレス５１から動的に生成される。

ＭＡＣアドレス５１は、ＣＥ機器９に固有の情報である。そして、固有鍵２３もＣＥ機器９に固有の鍵情報となるように構成されている。

本実施の形態では、一例としてＭＡＣアドレス５１を用いて固有鍵２３を生成するが、この他に、ｉ．Ｌｉｎｋ（ＩＥＥＥ１３９４）のアドレスなど、ＣＥ機器９に固有な情報であればよい。

【００２２】

即ち、ＣＥ機器９に固有な情報を用いて、ＣＥ機器９に固有な固有鍵２３が生成されるようになっている。

このように、製造される各ＣＥ機器９に組み込む固有鍵生成子２２が共通であっても、生成される固有鍵２３は、各ＣＥ機器９に固有なものとなり、固有鍵生成子２２の管理が容易になる。

このように構成された認証モジュール２０は、機器認証時に認証情報メモリ４０から機器認証情報を読み出して復号化し、機器ＩＤ４１と共に機器認証サーバ８に送信する。

固有鍵２３は、使用された後、所定期間内に速やかに消去される。所定期間は、例えば、機器認証情報を復号化してから機器認証部９９が機器認証を終えるまでなど、各種の設定が可能である。

なお、本実施の形態では、固有鍵２３は、使用後に消去されるように構成したが、必ずしも消去する必要はない。

【００２３】

書込モジュール３０は、工場５でＣＥ機器９に機器認証情報を書き込むための機能部である。

書込モジュール３０は、書込前鍵３１、固有鍵生成子３２、機器側確認ハッシュ関数３４、サーバ側確認ハッシュ関数３５などを備えている。

書込前鍵３１は、管理センタ３から送信されてきた暗号化された機器認証情報を復号化するための鍵情報である。

固有鍵生成子３２は、固有鍵３３を生成するための元（シード）となる情報であり、認証モジュール２０の固有鍵生成子２２と同じものである。

【００２４】

固有鍵３３は、書込前鍵３１によって復号化された機器認証情報を暗号化するための鍵情報であり、固有鍵生成子３２と、ＭＡＣアドレス５１から使用時に動的に生成される。固有鍵３３は、認証モジュール２０で生成される固有鍵２３と同じものである。

このように構成された書込モジュール３０は、管理センタ３から送信されてきた機器認証情報を書込前鍵３１で復号化し、固有鍵３３で再度暗号化して認証情報メモリ４０に記憶する。

【００２５】

本実施の形態では、機器認証情報を固有鍵３３にて暗号化された状態で記憶することによりセキュリティを高めている。

なお、書込前鍵３１で復号化した機器認証情報を暗号化せずに記憶装置に記憶するように構成することもできる。この場合は、認証モジュール２０は、認証時に機器認証情報を復号化する必要がないので固有鍵２３を生成する必要はない。

【００２６】

機器側確認ハッシュ関数３４は、機器認証情報が適切に認証情報メモリ４０に記憶されたことを書込モジュール３０が確認するための関数である。後述するように、書込モジュール３０は、管理センタ３から送信されてきたハッシュ値と、機器側確認ハッシュ関数３４による機器認証情報のハッシュ値を比較することにより機器認証情報が組み込まれたことを確認する。

【００２７】

サーバ側確認ハッシュ関数３５は、機器認証情報が適切に認証情報メモリ４０に記憶されたことを管理センタ３側が確認するための関数である。

後述するように、書込モジュール３０は、認証情報メモリ４０に記憶した機器認証情報のサーバ側確認ハッシュ関数３５によるハッシュ値を管理センタ３に送信する。

これに対し、管理センタ３は、発行した機器認証情報のサーバ側確認ハッシュ関数によるハッシュ値を生成し、書込モジュール３０から取得したハッシュ値と比較することにより、機器認証情報がＣＥ機器９に組み込まれたことを確認する。

【００２８】

本実施の形態では、ＣＥ機器９側で確認するための機器側確認ハッシュ関数３４と、管理サーバ７側手確認するためのサーバ側確認ハッシュ関数３５の２種類を用意した。

仮に、同じハッシュ関数を用いてＣＥ機器９側での確認と管理サーバ７側での確認を行うとすると、管理サーバ７がＣＥ機器９に送信したハッシュ値を第三者がそのまま管理サーバ７に返送した場合、管理サーバ７が、このハッシュ値がＣＥ機器９から送信されたものか、あるいは第三者から返送されたものか確認するのが困難である。

そのため、２種類のハッシュ関数を用いることにより、第三者によるなりすましを防止することができる。

【００２９】

ところで、ハッシュ関数とは、電子文書をハッシュ化するための関数であり、電子文書をハッシュ化することにより電子文書から電子文書に固有な文字列（ハッシュ値、又はダイジェストメッセージとも呼ばれる）を生成することができる。

同じ電子文書からは同じハッシュ値が得られる。電子文書が一部でも変更されると、この文書のハッシュ値は、変更前のものと異なる。

更に、ハッシュ値を逆変換して元の電子文書を得ることは大変困難である。

このように、ハッシュ関数は、順方向の変換は容易であるが、変換後の値から元の値を

得る逆変換が困難である一方向性関数と呼ばれる関数の一種である。

このように、秘密情報の確認する側と確認される側の双方で秘密情報のハッシュ値を生成し、これを比較することにより秘密情報の秘密状態を保ったまま、秘密情報の同一性を確認することができる。

【００３０】

認証情報メモリ４０は、機器認証情報などの機器認証を行う際に使用する情報を記憶する記憶装置である。

本実施の形態では、認証情報メモリ４０には、機器ＩＤ４１、暗号化（機器ＩＤ＋パスフレーズ）４２が記憶されている。

機器ＩＤ４１は、ＣＥ機器９を識別するためのＩＤ情報であって、工場５が機器ＩＤ管理機関から予め取得し、ＣＥ機器９に書き込んだものである。

暗号化（機器ＩＤ＋パスフレーズ）４２は、機器ＩＤ４１の後尾にパスフレーズを配置したものを固有鍵２３、又は固有鍵３３で暗号化したものである。なお、配置の順序は、逆でもよい。

以降、ある情報Ａの後尾にある情報Ｂを配置した情報を（情報Ａ＋情報Ｂ）などと表すことにし、更に（情報Ａ＋情報Ｂ）を暗号化した情報を暗号化（情報Ａ＋情報Ｂ）などと表すことにする。

【００３１】

例えば、機器ＩＤ４１を「１２３」とし、パスフレーズを「ａｂｃ」とした場合、（機器ＩＤ＋パスフレーズ）は、「１２３ａｂｃ」となる。そして、これを固有鍵２３、又は固有鍵３３で暗号化したものが暗号化（機器ＩＤ＋パスフレーズ）４２となる。

パスフレーズは、工場５がＣＥ機器９に機器認証情報を組み込む際に管理サーバ７が発行した秘密情報である。

本実施の形態では、（機器ＩＤ＋パスフレーズ）を機器認証情報として使用する。

このように、パスフレーズに機器ＩＤを組み合わせることにより機器認証情報のデータ量が多くなるため、第三者による暗号化（機器ＩＤ＋パスフレーズ）４２の解読が困難となり、セキュリティを高めることができる。

また、復号化された（機器ＩＤ＋パスフレーズ）と、送られてくる機器ＩＤをＣＥ機器９内で比較することにより、機器ＩＤと暗号化（機器ＩＤ＋パスフレーズ）の組合せが正しいことを検証することもできる。

【００３２】

本体識別情報メモリ５０は、ＣＥ機器９の本体を識別するための情報が記憶されている。

本体を識別するための情報としては、ネットワーク上でＣＥ機器９を識別するためのＣＥ機器９に固有な情報であるＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）アドレス５１や、ｉＬｉｎｋなどと呼ばれる情報などがある。

ＭＡＣアドレス５１は、ＣＥ機器９にユニークなハードウェアアドレスであって、例えネットワーク上でＣＥ機器９を移動したとしても変わらない。

【００３３】

次に、以上のように構成されたＣＥ機器９に機器認証情報を組み込む手順、組み込んだ機器認証情報を確認する手順、組み込んだ機器認証情報を用いて機器認証を行う手順についてフローチャートを用いて説明する。

【００３４】

図４は、ＣＥ機器９に機器認証情報を組み込む準備段階での作業手順を説明するためのフローチャートである。

まず、事業体１１がＣＥ機器９を企画する（ステップ１０）。この作業は、企画担当者などの人手により行われるものである。

次に、事業体１１に設置された事業体システムから管理サーバ７にアクセスし、ＣＥ機器９の書込モジュール３０に組み込むための書込前鍵３１を要求する（ステップ１２）。

【００３５】

管理サーバ７は、図８に示したような鍵テーブル７００を備えており、鍵テーブル７００から書込前鍵３１とこの書込前鍵３１を他の書込前鍵から識別する鍵識別子を発行する。そして発行した書込前鍵３１と鍵識別子を共に事業体システムに送信する（ステップ２０）。

また、事業体１１は、製品の機種を特定する製品コードと後述する固有鍵生成子を管理サーバに要求するように構成することもできる。

管理サーバ７は、製品コードと固有鍵生成子が対応付けて管理している。

【００３６】

事業体システムは、管理サーバ７から書込前鍵３１と鍵識別子を受信し、書込前鍵３１を書込モジュール３０に組み込むように構成されたファームウェアを作成する（ステップ１４）。また、後述する固有鍵生成子もファームウェアに組み込む。

次に、事業体システムは、作成したファームウェアと鍵識別子、及びＣＥ機器９の機種を特定する製品コードを工場５に設置された工場システムに送信する（ステップ１６）。

なお、工場５では、製品コードで特定されるＣＥ機器９を複数台生産するが、何れのＣＥ機器９も同じ書込前鍵３１を使用するものとする。そのため、ファームウェアと鍵識別子は一組工場に送信され、この一組のファームウェアと鍵識別子から複数台のＣＥ機器９が生産される。

【００３７】

工場システムは、事業体システムからこれらの情報を受信する。そして工場５は、受信した製品コードで特定されるＣＥ機器９の製造を開始する。

このようにして製造されたのＣＥ機器９（ファームウェア組み込み前）に対して工場システムは製品シリアル番号を発番する（ステップ３０）。

製品シリアル番号は、個々のＣＥ機器９に対して固有な番号であり、例えば、ラベルシールに数字やバーコードなどとして印刷され、ＣＥ機器９に外部から参照可能に貼付される。

【００３８】

なお、本実施の形態では、製品シリアル番号がＣＥ機器９を特定できる情報であるとするが、例えば、製品コードと製品シリアル番号を用いてＣＥ機器９を特定できるように構成することもできる。

この場合は、機器認証サーバ８は、製品コードと製品シリアル番号をＣＥ機器９に貼付する。

即ち、ＣＥ機器９を特定できる情報であればよい。

【００３９】

次に、工場システムは、ＣＥ機器９にファームウェアを組み込む（ステップ３２）。

ファームウェアの組み込みは、ＣＥ機器９のコネクタからファームウェアを入力することにより行われる。

また、事業体１１がファームウェアをＣＤ－ＲＯＭなどの記憶媒体に記憶させて工場５に送付し、工場５でこれをＣＥ機器９に読み込ませるように構成することもできる。

【００４０】

ファームウェアの組み込みにより、機器認証部９９（図３）がＣＥ機器９の内部に形成される。

なお、工場システムは、ファームウェア組み込みの際に、予め機器ＩＤ管理機関から取得しておいた機器ＩＤ４１を認証情報メモリ４０に記憶させる。ただし、この段階では認証情報メモリ４０には暗号化（機器ＩＤ＋パスフレーズ）４２は記憶されていない。

【００４１】

図５は、ＣＥ機器９に機器認証情報を組み込む（埋め込む）手順（即ち、認証情報メモリ４０に暗号化（機器ＩＤ＋パスフレーズ）４２を記憶させる手順）を説明するためのフローチャートである。

なお、以下の処理は、ＣＥ機器９に接続手段１０が接続された状態で行う。

【００４２】

工場システムは、図８に示したような鍵識別子管理テーブル５００を備えており、製品（製品コード）と事業体システムから取得した鍵識別子を対応付けて管理している。

そして、工場システムは、管理サーバ７にアクセスし、パスフレーズの発行を要求すると共に、先に取得した機器ＩＤ４１と鍵識別子管理テーブル５００に記憶されているＣＥ機器９の鍵識別子を送信する（ステップ４０）。

【００４３】

管理サーバ７は、パスフレーズの発行要求を受けてパスフレーズを発行する（ステップ５０）。

なお、パスフレーズとは、文字や数字、あるいは記号などの文字列からなる秘密情報であって、パスワードと同種の情報である。

このような秘密情報のうち、文字列の比較的短いものをパスワードと呼び、比較的長いものをパスフレーズと呼んでいる。暗号化した場合に、文字列が長いほど第三者による解読が困難になる。

【００４４】

次に、管理サーバ７は、工場システムから受信した鍵識別子に対応する書込前鍵３１を鍵テーブル７００（図８）から取得する。

そして、工場システムから受信した機器ＩＤ４１とステップ５０で発行したパスフレーズから（機器ＩＤ＋パスフレーズ）を生成し、先に取得した書込前鍵３１にてこれを暗号化して暗号化（機器ＩＤ＋パスフレーズ）４２を生成する（ステップ５２）。

この暗号化（機器ＩＤ＋パスフレーズ）が機器認証情報として使用される。

【００４５】

管理サーバ７は、ＣＥ機器９と同様に、機器側確認ハッシュ関数３４と、サーバ側確認ハッシュ関数３５を備えており、機器側確認ハッシュ関数３４を用いて先に生成した（機器ＩＤ＋パスフレーズ）のハッシュ値（第１のハッシュ値）を生成する（ステップ５４）。

この第１のハッシュ値は、機器認証情報が適切に組み込まれたか否かをＣＥ機器９内部で判断する際に使用される。

なお、サーバ側確認ハッシュ関数３５は、後に、ＣＥ機器９に機器認証情報が適切に組み込まれたか否かを管理サーバ７が判断する際に使用される。

【００４６】

管理サーバ７は、機器ＩＤ４１、生成した暗号化（機器ＩＤ＋パスフレーズ）４２、及び第１のハッシュ値を工場システムに送信する（ステップ５６）。これは、元情報提供手段に対応する。

なお、管理サーバ７は、図８に示した発行済み機器認証情報テーブル７０２を記憶しており、機器ＩＤ４１、暗号化（機器ＩＤ＋パスフレーズ）４２、第１のハッシュ値を工場システムに送信すると共に、発行済み機器認証情報テーブル７０２を更新する。

これにより、発行したパスフレーズと、機器ＩＤ４１、鍵識別子を対応付けることができる。

【００４７】

工場システムは、これらの情報を管理サーバ７から受信し、これらの情報を接続手段１０を介してＣＥ機器９に入力する（ステップ４２）。

すると、ＣＥ機器９内部では、書込モジュール３０がこれらの情報を受信する（ステップ６０）。これは、暗号化（機器ＩＤ＋パスフレーズ）４２は、元情報に対応し、そのため書込モジュール３０は、元情報取得手段を備えている。

また、第１のハッシュ値は、機器認証情報を一方向性関数で変換した変換値に対応し、そのため、書込モジュール３０は、変換値取得手段を備えている。

【００４８】

次に、書込モジュール３０は、書込前鍵３１を用いて暗号化（機器ＩＤ＋パスフレーズ）４２を復号化する（ステップ６２）。

この復号化により、ＣＥ機器９は、管理センタ３から取得した機器認証情報、即ち（機

器ＩＤ＋パスフレーズ）を得ることができる。
　このように、書込モジュール３０は、元情報から機器認証情報を生成する生成手段を有している。
【００４９】
　ＣＥ機器９は、復号化した（機器ＩＤ＋パスフレーズ）をそのまま保持してもよいが、本実施の形態では、セキュリティを高めるため、（機器ＩＤ＋パスフレーズ）を再度暗号化して保持することにする。
　そのため、書込モジュール３０は、まず、ＭＡＣアドレス５１と固有鍵生成子３２から固有鍵３３を生成する（ステップ６４）。
　このステップは、ＣＥ機器９に固有の暗号化鍵を得ることが目的であって、一例としてＭＡＣアドレス５１を用いて固有鍵３３を生成するが、これに限定するものではなく、ＣＥ機器９に固有の情報であれば（例えば、製品シリアル番号）何でもよい。
　また、後述するように、認証モジュール２０も固有鍵３３と同じ暗号化鍵を生成することができ、書込モジュール３０、認証モジュール２０は、共に鍵生成手段を有している。
【００５０】
　次に、書込モジュール３０は、生成した固有鍵３３を用いて（機器ＩＤ＋パスフレーズ）を暗号化して暗号化（機器ＩＤ＋パスフレーズ）４２を生成する（ステップ６６）。
　なお、暗号化に使用する暗号鍵が異なるので、暗号化（機器ＩＤ＋パスフレーズ）４２と、管理サーバ７が送信してきた暗号化（機器ＩＤ＋パスフレーズ）は、異なるものである。
【００５１】
　次に、書込モジュール３０は、生成した暗号化（機器ＩＤ＋パスフレーズ）４２を認証情報メモリ４０に書き込み（ステップ６８）、認証情報メモリ４０は、
暗号化（機器ＩＤ＋パスフレーズ）４２を記憶する（ステップ７０）。
　なお、固有鍵３３は、機器認証部９９が固有鍵３３を消去するように構成されている場合は、使用された後、速やかに消去される（鍵消去手段）。
　このように、暗号化（機器ＩＤ＋パスフレーズ）４２は、ＣＥ機器９に固有であり、しかも動的に生成される固有鍵３３により暗号化されているので、セキュリティを高めることができる。
　また、認証情報メモリ４０は、記憶手段を構成している。
【００５２】
　以上の手順により、管理サーバ７が発行した機器認証情報をＣＥ機器９に組み込むことができる。
　更に、機器認証情報は、暗号化された状態のままＣＥ機器９に入力されるので、機器認証情報が工場５で漏出することを未然に防ぐことができ、機器認証情報組み込み時のセキュリティを高めることができる。
　更に、機器認証情報は、ＣＥ機器９に固有な暗号鍵で暗号化した状態でＣＥ機器９に記憶されるので、ＣＥ機器９を出荷した後にＣＥ機器９から機器認証情報が漏出することを未然に防ぐことができ、出荷後のセキュリティも高めることができる。
【００５３】
　図６は、ＣＥ機器９に機器認証情報が適切に組み込まれたことを管理センタ３、及び工場５が確認する手順を説明するためのフローチャートである。
　この手順は、ＣＥ機器９のコネクタに接続手段１０が接続した状態で行われる。通常は、工場システムがＣＥ機器９に機器認証情報を組み込んだ後、自動的に行われる。
【００５４】
　まず、機器認証部９９において、書込モジュール３０が認証情報メモリ４０から暗号化（機器ＩＤ＋パスフレーズ）４２を読み出し、認証情報メモリ４０から書込モジュール３０へ暗号化（機器ＩＤ＋パスフレーズ）４２が提供される（ステップ９０）。
　次に、書込モジュール３０は、固有鍵生成子３２と、ＭＡＣアドレス５１から固有鍵３３を生成し（ステップ１００）、これを用いて暗号化（機器ＩＤ＋パスフレーズ）４２を

復号化する（ステップ１０２）。

【００５５】

次に、書込モジュール３０は、機器側確認ハッシュ関数３４を用いて、復号化した（機器ＩＤ＋パスフレーズ）のハッシュ値（第１のハッシュ値）を生成する（ステップ１０４）。

次に、書込モジュール３０は、管理サーバ７から送信されてきた第１のハッシュ値と、ステップ１０４で生成したハッシュ値を比較し、これらのハッシュ値が一致するか否かの比較結果を得る（ステップ１０６）。

このように、書込モジュール３０は、変換値（第１のハッシュ値）算出手段と、判断手段を備えている。

【００５６】

ハッシュ値が一致することにより、管理サーバ７が生成した（機器ＩＤ＋パスフレーズ）が、認証情報メモリ４０に記憶されている（機器ＩＤ＋パスフレーズ）と同一のものであることを確認することができる。

【００５７】

次に、書込モジュール３０は、サーバ側確認ハッシュ関数３５を用いて（機器ＩＤ＋パスフレーズ）のハッシュ値（第２のハッシュ値）を生成する（ステップ１０８）。

そして、書込モジュール３０は、認証情報メモリ４０から機器ＩＤ４１を読み出し、ステップ１０６における第１のハッシュ値の比較結果、機器ＩＤ、第２のハッシュ値を工場システムに出力する（ステップ１１０）。そして、第２のハッシュ値は、管理サーバ７に送信される。

このように、書込モジュール３０は、変換値算出手段と、変換値提供手段を備えている。

【００５８】

工場は、ＣＥ機器９から出力された比較結果により、機器認証情報がＣＥ機器９に適切に組み込まれたか否かを知ることができる。

ハッシュ値が一致しなかった場合は、機器ＩＤ４１を廃棄し、新たな機器ＩＤを採用して再度機器認証情報の組み込みを試みる。

組み込みに失敗した機器ＩＤ４１を再度利用することも可能であるが、手違いなどにより同じ機器ＩＤのＣＥ機器９が複数市場に出回るのを防止するため、本実施の形態では、組み込みに失敗した機器ＩＤ４１は廃棄するものとした。

【００５９】

なお、従来の製造工程では、機器認証情報の機密性を保つため、一端ＣＥ機器９に組み込んだ後は、適切に機器認証情報が組み込まれたか否かを調べることは困難であり、確認を行わない場合もあった。

しかし、本実施の形態では、機器認証情報のハッシュ値をＣＥ機器９内部で比較することにより、機器認証情報の機密性をＣＥ機器９内部で保ったまま機器認証情報が組み込まれたか否かを調べることができる。

【００６０】

工場システムは、機器認証情報が適切にＣＥ機器９に組み込まれたことを確認した後、ＣＥ機器９から得た機器ＩＤ４１と第２のハッシュ値に、ＣＥ機器９の製品シリアル番号を付加して管理サーバ７に送信する（ステップ１２０）。

【００６１】

管理サーバ７は、これらの情報を工場システムから受信し、発行済み機器認証情報テーブル７０２（図８）を用いて機器ＩＤ４１からパスフレーズを検索する（ステップ１３０）。

このように、管理サーバ７は、変換値（第２のハッシュ値）取得手段を備えている。

次に、管理サーバ７は、機器ＩＤ４１と検索したパスフレーズから（機器ＩＤ＋パスフレーズ）を生成し、これからサーバ側確認ハッシュ関数３５を用いて第２のハッシュ値を生成する（変換値算出手段）。

【００６２】
そして、工場システムから受信した第２のハッシュ値と、先に生成した第２のハッシュ値が一致するか否かを判断する（判断手段）（ステップ１３２）。
第２のハッシュ値が一致することにより、管理サーバ７は、ＣＥ機器９に対する機器認証情報の組み込みが成功したことを知ることができる。
逆に第２のハッシュ値が一致しなかった場合、機器認証情報の組み込みが失敗したことを知ることができる。
【００６３】
管理サーバ７は、図８に示したような機器認証テーブル７０４を備えており、機器ＩＤ４１、パスフレーズ、製品シリアル番号を対応付けて記憶している。
第２のハッシュ値が一致した場合、管理サーバ７は、機器ＩＤ４１と製品シリアル番号をパスフレーズと共に紐付けて機器認証テーブル７０４に記憶する（ステップ１３４）。
なお、機器認証テーブル７０４は、機器認証サーバ８に提供され、機器認証サーバ８が機器認証を行うのに利用される（機器認証情報提供手段）。
【００６４】
次に、管理サーバ７は、工場システムから受信したデータ（機器ＩＤ４１、製品シリアル番号、第２のハッシュ値）に、データを受信した日の日付情報を付加して秘密鍵で署名（電子署名）して工場に送信する（判断結果送信手段）（ステップ１３６）。
工場システム（元情報組込主体）は、これを受信し、機器認証情報が適切にＣＥ機器９に組み込まれたことを確認する（ステップ１２２）。
これにより、工場システム側では、管理サーバ７に機器ＩＤ４１、製品シリアル番号、第２のハッシュ値（これらを以て製造実績とすることができる）を受け取ってもらえたことを確認することができる。
そして、工場５は、製造が完了したＣＥ機器９を出荷する。
【００６５】
図７は、機器認証サーバ８がＣＥ機器９を機器認証する手順を説明するためのフローチャートである。
まず、機器認証部９９（図３）の認証モジュール２０が、認証情報メモリ４０から暗号化（機器ＩＤ＋パスフレーズ）４２を読み出し、認証情報メモリ４０から認証モジュール２０に暗号化（機器ＩＤ＋パスフレーズ）４２が提供される（ステップ１４０）。
【００６６】
次に、認証モジュール２０は、固有鍵生成子２２とＭＡＣアドレス５１を用いて固有鍵２３を生成する（ステップ１５０）。
そして認証モジュール２０は、暗号化（機器ＩＤ＋パスフレーズ）４２を固有鍵２３を用いて復号化して（機器ＩＤ＋パスフレーズ）を取得し（ステップ１５２）、機器認証サーバ８に送信する（ステップ１５４）。このように、認証モジュール２０は、機器認証情報送信手段を備えている。
なお、ＣＥ機器９と機器認証サーバ８の間の通信経路は、例えば、ＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔｓ　Ｌａｙｅｒ）などの暗号化技術を使ってセキュアなものとなっている。
【００６７】
機器認証サーバ８は、ＣＥ機器９から（機器ＩＤ＋パスフレーズ）を受信し、これを公開鍵２１に対応する秘密鍵で復号化し、管理センタ３から提供された機器認証テーブル７０４のパスフレーズと照合してＣＥ機器９を機器認証する（ステップ１６０）。
更に、機器認証テーブル７０４を用いてＣＥ機器９の製品シリアル番号を特定する（ステップ１６２）。
以上の手順により機器認証処理は行われる。
【００６８】
図９は、ＣＥ機器９のハードウェア的な構成の一例を示した図である。
ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）１２１は、ＲＯＭ（Ｒｅ

ａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）１２２に記憶されているプログラムや、記憶部１２８からＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）１２３にロードされたプログラムに従って各種の処理を実行する中央処理装置である。

【００６９】

ＲＯＭ１２２は、ＣＥ機器９を機能させる上で必要な基本的なプログラムやパラメータなどから構成されている。

ＲＡＭ１２３は、ＣＰＵ１２１が各種の処理を実行する上で必要なワーキングエリアを提供する。

【００７０】

記憶部１２８は、ＣＥ機器９が機能するために必要な各プログラムやデータを記憶しており、例えば、ハードディスクや半導体メモリなどの記憶装置により構成されている。

事業体１１で作成されたファームウェアは、工場５で記憶部１２８に記憶され、このファームウェアがＣＰＵ１２１で実行されることにより、機器認証部９９（図３）の各構成要素が生成される。

記憶部１２８に記憶されている他のプログラムとしては、ファイルの入出力を行ったり、ＣＥ機器９の各部を制御したりなど、基本的な機能を実現するためのＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）などがある。

【００７１】

ＣＰＵ１２１、ＲＯＭ１２２、及びＲＡＭ１２３は、バス１２４を介して相互に接続されている。このバス１２４には、入出力インターフェース１２５も接続されている。

入出力インターフェース１２５には、キーボード、マウスなどよりなる入力部１２６、ＣＲＴ（Ｃａｔｈｏｄｅ－ｒａｙ　Ｔｕｂｅ）、ＬＣＤ（Ｌｉｑｕｉｄ　Ｃｒｙｓｔａｌ　Ｄｉｓｐｌａｙ）などよりなるディスプレイ、並びにスピーカなどによりなる出力部１２７、ハードディスクなどにより構成される記憶部１２８、モデム、ターミナルアダプタなどにより構成される通信部１２９が接続されている。

通信部１２９は、ネットワークを介しての通信処理を行う機能部であり、例えば、接続手段１０と接続して機器認証情報の入力を受け付けたり、あるいは、機器認証サーバ８と接続して機器認証を行うための通信を行ったりする。

【００７２】

また、入出力インターフェース１２５には、必要に応じてドライブ１３０が接続され、磁気ディスク１４１、光ディスク１４２、光磁気ディスク１４３、又はメモリカード１４４などが適宜装着され、それから読み出されたコンピュータプログラムが、必要に応じて記憶部１２８にインストールされる。

なお、管理サーバ７、機器認証サーバ８の構成は基本的にＣＥ機器９と同様であるので説明は省略する。

【００７３】

以上に説明した第１の実施の形態により、機器認証の際に必要となる機器認証情報（機器ＩＤ＋パスフレーズ）を、管理サーバ７からＣＥ機器９へ安全に送信することができる。また、機器認証情報が正しく書き込まれたことを工場５や管理サーバ７が確認することが可能となる。

【００７４】

以上に説明した第１の実施の形態による効果を従来の問題点と対比しながら列挙すると以下のようになる。

（１）従来は、機器認証情報である（機器ＩＤ＋パスフレーズ）が平文でＣＥ機器９入力されていたため、意図の如何に関わらず工場５の作業者などの目に触れてしまう可能性があった。これに対し、本実施の形態では、この問題を（機器ＩＤ＋パスフレーズ）を暗号化したままＣＥ機器９に入力することにより対応した。

【００７５】

（２）従来は、例え機器認証情報を暗号化して工場５に送信したとしても、製品ごと、工場ごとに機器認証情報の組み込み方式の統一が取れず、セキュリティレベルのばらつきを

生んでしまう可能性があった。これに対し、本実施の形態では、機器認証情報の組み込み方式を共通化することにより、セキュリティレベルのばらつきを軽減することができる。
（３）従来は、暗号化鍵が漏出することにより他のＣＥ機器９に影響が及ぶ場合があった。これに対し、本実施の形態では、ＣＥ機器９ごとに固有な固有鍵２３を生成することにより例え固有鍵２３が漏出したとしても他のＣＥ機器９に影響が及ぶことはない。
また、書込前鍵３１に関しては、鍵の単位を製品ごとや時期ごとなどにすることで影響範囲を限定することができる。

【００７６】

（４）従来は、ＣＥ機器９内に正しく機器認証情報が書き込まれたことを工場５や、機器認証情報の発行元である管理センタ３が確認するのは困難であった。これに対し、本実施の形態では、ハッシュ値などの固有情報を使って工場５や管理センタ３が機器認証情報が正しく組み込まれたことを確認することができる。
（５）従来は、管理センタ３が、正しく実績報告を受け取ったことを工場５が確認することは困難であった。これに対し、本実施の形態では、管理サーバ７が工場システムから受信したデータに日時情報を付加して電子署名し、これを工場システムに送信するようにした。
（６）従来は、機器認証情報として、電子証明書などの他の情報を用いることは困難であった。これに対し本実施の形態は、電子証明書を使った認証方式にも適用することができる。

【００７７】

なお、本実施の形態では、一例として、機器認証情報をネットワーク経由で工場５に送信して接続具１０からＣＥ機器９に入力したが、機器認証情報は暗号化したままＣＥ機器９に入力されるので、例えば、ＣＤ－ＲＯＭなどの記憶媒体に記憶して工場５に送付し、工場５において記憶媒体からＣＥ機器９に機器認証情報を書き込むように構成してもよい。
更に、本実施の形態では、一例として、管理サーバ７から送信されてきた暗号化（機器ＩＤ＋パスフレーズ）を書込前鍵で複合化した後に認証情報メモリ４０に記憶するように構成したが、この他に、管理サーバ７から送信されてきた暗号化（機器ＩＤ＋パスフレーズ）を復号化せずに認証情報メモリ４０に記憶し、機器認証時に書込前鍵で復号化するように構成することもできる。

【００７８】

次に、第２の実施の形態について説明する。
［第２の実施の形態の概要］
図１０は、第２の実施の形態の概要を説明するための図である。
本実施の形態では、機器認証情報を生成する元となる元情報を管理サーバ７とＣＥ機器９で同じロジックを用いて（例えば、同じ暗号鍵を用いて同じ暗号方式により暗号化して）変換し、機器認証情報を生成する。

【００７９】

まず、管理サーバ７は、元情報を工場５に送信すると共に、元情報を変換して機器認証情報を生成する。
一方、工場５では、接続手段１０を介して元情報をＣＥ機器９に入力する。ＣＥ機器９は、入力された元情報を変換して機器認証情報を生成する。
以上のようにして、管理サーバ７とＣＥ機器９は、機器認証情報を共有することかできる。
また、仮に元情報が外部に漏出したとしてもロジックを知らなければ機器認証情報を知ることはできない。

【００８０】

以上のように、機器認証情報は、ＣＥ機器９の内部で生成されるため、工場５において、平文で出力されるのを防ぐことができる。

【００８１】

［第２の実施の形態の詳細］

製造認証システム１の構成（図２）、及び機器認証部９９（図３）は、第１の実施の形態と同様であるので説明を省略する。

また、第１の実施の形態と同じ構成要素には同じ符号を付して説明する。

以下に、ＣＥ機器９への機器認証情報の組み込み、組み込みの確認、及び機器認証の方法についてフローチャートを用いて説明する。

なお、ＣＥ機器９に機器認証情報を組み込む前準備は、第１の実施の形態と同様であるので（図４）説明を省略する。

管理サーバ７は、第１の実施の形態と同様に、図１４に示したような鍵テーブル７０６を備えており、鍵識別子と書込前鍵３１を対応付けて管理している。

【００８２】

図１１は、ＣＥ機器９に機器認証情報を組み込む手順を説明するためのフローチャートである。

ＣＥ機器９は、既に組み立てがなされており、コネクタに接続手段１０が接続された状態になっているものとする。

まず、工場システムは、管理サーバ７に対してパスフレーズの発行を要求すると共に、予め機器ＩＤ管理機関から取得しておいた機器ＩＤ４１を管理サーバ７に送信する（ステップ２００）。

なお、この機器ＩＤ４１は認証情報メモリ４０にも記憶させる。

【００８３】

これに対して、管理サーバ７は、パスフレーズを発行する（ステップ２１０）。

管理サーバ７は、図１４に示したような発行済み機器認証情報テーブル７０８を備えており、工場システムから受信した機器ＩＤ４１と、この機器ＩＤ４１に対して発行したパスフレーズを対応付けて記憶している。

そして、管理サーバ７は、パスフレーズを発行した後、機器ＩＤ４１とパスフレーズを紐付けて発行済み機器認証情報テーブル７０８に記憶する（ステップ２１２）。

【００８４】

次に、管理サーバ７は、機器ＩＤ４１とパスフレーズから（機器ＩＤ＋パスフレーズ）を生成し、工場システムに送信する（ステップ２１４）。

この（機器ＩＤ＋パスフレーズ）が機器認証情報を生成するための元情報となる。

工場システムは、管理サーバ７から（機器ＩＤ＋パスフレーズ）を受信し（ステップ２０２）、接続手段１０を介してＣＥ機器９に入力する（ステップ２０４）。

【００８５】

ＣＥ機器９内部では、書込モジュール３０が（機器ＩＤ＋パスフレーズ）を受信し（ステップ２２０）、書込前鍵３１を用いてこれを暗号化して暗号化（機器ＩＤ＋パスフレーズ）４２を生成する（ステップ２２２）。

本実施の形態では、（機器ＩＤ＋パスフレーズ）を元情報として暗号化（機器ＩＤ＋パスフレーズ）４２を生成し、暗号化（機器ＩＤ＋パスフレーズ）４２を機器認証情報として使用する。

即ち、（機器ＩＤ＋パスフレーズ）を、書込前鍵３１を用いた変換式により変換し、変換後の値である暗号化（機器ＩＤ＋パスフレーズ）４２を機器認証情報として使用する。

【００８６】

次に、書込モジュール３０は、固有鍵生成子３２とＭＡＣアドレス５１から固有鍵３３を生成し（ステップ２２４）、生成した固有鍵３３によって、暗号化（機器ＩＤ＋パスフレーズ）４２を再度暗号化する（ステップ２２６）。

これは、本実施の形態では、暗号化（機器ＩＤ＋パスフレーズ）４２を機器認証情報として使用するため、これを更に暗号化された状態でＣＥ機器９に保持することによりセキュリティを高めるものである。

以降、暗号化（情報Ａ＋情報Ｂ）を再度暗号化したものを再度暗号化（情報Ａ＋情報Ｂ）などと記すことにする。

【００８７】
書込モジュール３０は、このようにして生成した再度暗号化（機器ＩＤ＋パスフレーズ）４２（再度暗号化（機器ＩＤ＋パスフレーズ）４２ａとする）を認証情報メモリ４０に書き込み（ステップ２２８）、認証情報メモリ４０は、再度暗号化（機器ＩＤ＋パスフレーズ）４２ａを記憶する（ステップ２３０）。
このように、本実施の形態では、認証情報メモリ４０に機器ＩＤ４１と、再度暗号化（機器ＩＤ＋パスフレーズ）４２ａが記憶されている。
【００８８】
図１２は、ＣＥ機器９に機器認証情報が適切に組み込まれたことを管理センタ３、及び工場５が確認する手順を説明するためのフローチャートである。
この手順は、ＣＥ機器９のコネクタに接続手段１０が接続した状態で行われる。通常は、工場システムがＣＥ機器９に機器認証情報を組み込んだ後、自動的に行われる。
【００８９】
まず、書込モジュール３０が認証情報メモリ４０から再度暗号化（機器ＩＤ＋パスフレーズ）４２ａを読み出し、認証情報メモリ４０から書込モジュール３０へ再度暗号化（機器ＩＤ＋パスフレーズ）４２ａが提供される（ステップ２４０）。
次に、書込モジュール３０は、固有鍵生成子３２と、ＭＡＣアドレス５１から固有鍵３３を生成し（ステップ２５０）、これを用いて再度暗号化（機器ＩＤ＋パスフレーズ）４２ａを複合化し、暗号化（機器ＩＤ＋パスフレーズ）４２を得る（ステップ２５２）。
【００９０】
次に、書込モジュール３０は、サーバ側確認ハッシュ関数３５を用いて暗号化（機器ＩＤ＋パスフレーズ）４２から第２のハッシュ値を生成し（ステップ２５４）、工場システムに出力する（ステップ２５６）。
第１の実施の形態では、（機器ＩＤ＋パスフレーズ）から第２のハッシュ値を生成したが、第２の実施の形態では、暗号化（機器ＩＤ＋パスフレーズ）４２から第２のハッシュ値を生成する。
なお、第２の実施の形態では、第１のハッシュ値は利用しない。
工場システムは、ＣＥ機器９から出力された第２のハッシュ値に、機器ＩＤ４１、製品シリアル番号、鍵識別子を付加して管理サーバ７に送信する（ステップ２６０）。
【００９１】
管理サーバ７は、工場システムから受信した機器ＩＤ４１を発行済み機器認証情報テーブル７０８（図１４）で検索し、このＣＥ機器９に対して発行したパスフレーズを取得する（ステップ２７０）。
次に、管理サーバ７は、工場システムから受信した鍵識別子を鍵テーブル７０６で検索し、ＣＥ機器９に記憶されているのと同じ書込前鍵３１を取得する（ステップ２７２）。
【００９２】
次に、管理サーバ７は、工場システムから受信した機器ＩＤ４１と、ステップ２７０で検索したパスフレーズを用いて（機器ＩＤ＋パスフレーズ）を生成し、これをステップ２７２で検索した書込前鍵３１で暗号化して暗号化（機器ＩＤ＋パスフレーズ）４２を生成する（ステップ２７４）。
次に、管理サーバ７は、生成した暗号化（機器ＩＤ＋パスフレーズ）４２をサーバ側確認ハッシュ関数３５を用いてハッシュ化し、第２のハッシュ値を生成する（ステップ２７６）。
【００９３】
次に、管理サーバ７は、ステップ２７６で生成した第２のハッシュ値と、工場システムから受信した第２のハッシュ値の一致を比較することにより、ＣＥ機器９に機器認証情報が適切に組み込まれたことを確認する（ステップ２７８）。
【００９４】
管理サーバ７は、図１４に示したような機器認証テーブル７１０を備えており、機器ＩＤ４１、暗号化（機器ＩＤ＋パスフレーズ）４２（即ち、機器認証情報）、製品シリアル

番号、鍵識別子を対応付けて記憶している。

管理サーバ７は、第２のハッシュ値の比較により、機器認証情報がＣＥ機器９に適切に組み込まれたことを検知すると、この暗号化（機器ＩＤ＋パスフレーズ）４２に、機器ＩＤ４１、製品シリアル番号、鍵識別子を紐付けて機器認証テーブル７１０に記憶する（ステップ２８０）。

なお、機器認証テーブル７１０は、機器認証サーバ８に提供され、ＣＥ機器９を機器認証する際に利用される。

【００９５】

次に、管理サーバ７は、工場システムから受信したデータに、受信した日時の日時情報を付加して秘密鍵で電子署名し、工場システムに送信する（ステップ２８２）。

工場システムは、電子署名を確認し、機器認証情報がＣＥ機器９に適切に組み込まれたことを確認する（ステップ２６２）。

工場５は、機器認証情報が組み込まれたことを確認した後、ＣＥ機器９を市場に出荷する。

【００９６】

図１３は、機器認証サーバ８がＣＥ機器９を機器認証する手順を説明するためのフローチャートである。

まず、機器認証部９９（図３）の認証モジュール２０が、認証情報メモリ４０から再度暗号化（機器ＩＤ＋パスフレーズ）４２ａを読み出し、認証情報メモリ４０から認証モジュール２０に再度暗号化（機器ＩＤ＋パスフレーズ）４２ａが提供される（ステップ２９０）。

【００９７】

次に、認証モジュール２０は、固有鍵生成子２２とＭＡＣアドレス５１を用いて固有鍵２３を生成する（ステップ３００）。

そして認証モジュール２０は、再度暗号化（機器ＩＤ＋パスフレーズ）４２ａを固有鍵２３を用いて復号化して暗号化（機器ＩＤ＋パスフレーズ）４２を取得し（ステップ３０２）、公開鍵２１で暗号化して、機器ＩＤ４１と共に機器認証サーバ８に送信する（ステップ３０４）。

【００９８】

機器認証サーバ８は、ＣＥ機器９から暗号化（機器ＩＤ＋パスフレーズ）４２を受信し、これを公開鍵２１に対応する秘密鍵で復号化する。そして、管理センタ３から提供された機器認証テーブル７１０を機器ＩＤ４１で検索し、ＣＥ機器９の暗号化（機器ＩＤ＋パスフレーズ）４２を特定する。そして特定した暗号化（機器ＩＤ＋パスフレーズ）４２と、受信した暗号化（機器ＩＤ＋パスフレーズ）４２と照合してＣＥ機器９を機器認証する（ステップ３１０）。

更に、機器認証テーブル７１０を用いてＣＥ機器９の製品シリアル番号を特定する（ステップ３１２）。

以上の手順によりＣＥ機器９の機器認証が行われる。

【００９９】

以上に説明した第２の実施の形態による効果を従来の問題点と対比しながら列挙する。

（１）従来は、管理サーバ７に機器認証情報を要求する場合、ＣＥ機器９に埋め込まれている書込前鍵３１に応じた暗号化パスフレーズを要求する必要があった。しかし、本実施の形態では、ＣＥ機器９に埋め込まれている書込前鍵３１を意識しないで（機器ＩＤ＋パスフレーズ）を管理サーバ７に要求することができる。

【０１００】

（２）従来は、ＣＥ機器９の製造が停止した場合、取得しておいた（機器ＩＤ＋パスフレーズ）が無駄になってしまっていた。しかし、本実施の形態では、管理サーバ７から取得した（機器ＩＤ＋パスフレーズ）は、どのＣＥ機器でも利用できるため、（機器ＩＤ＋パスフレーズ）が余った場合は、他のＣＥ機器に融通することができる。

（３）従来は、ＣＥ機器９の製造ラインを考慮に入れると自由な書込前鍵３１の単位の設

定ができなかった。これに対し、本実施の形態では、製造ラインを気にすることなく書込前鍵３１の単位を設定することができる。

【０１０１】

なお、本実施の形態では、管理サーバ７で元情報、（即ち（端末ＩＤ＋パスフレーズ））から機器認証情報（即ち、暗号化（端末ＩＤ＋パスフレーズ））を生成し、機器認証サーバ８に提供したが、これに限定せず、管理サーバ７は元情報を機器認証サーバ８に提供し、機器認証サーバ８で元情報から機器認証情報を生成するように構成することもできる。

【０１０２】

[第３の実施の形態]

次に、第３の実施の形態について説明する。

この実施の形態は、機器認証情報を暗号化・復号化するための鍵情報が含まれているアプリケーション（機器認証クライアント）を更新するものである。

機器認証クライアントは、ＣＥ機器やパーソナルコンピュータなどにインストールされ、機器認証部９９（図３）と同様なモジュールが形成される。そして、モジュールに含まれる公開鍵（公開鍵２１に対応）は、使用期限などが設定されており、新規なものに更新する必要がある場合がある。

従来は、このような場合、機器認証クライアントを全て新しいものに交換する必要があった。

本実施の形態では、機器認証クライアントに含まれる機器認証部９９に対応するモジュールを新しいものに交換することにより、このモジュールに含まれる公開鍵の更新を行う。

【０１０３】

以下、ＣＥ機器９の機器認証部９９を更新する場合を例にとり、図１５のフローチャートを用いながら更新の手順を説明する。

なお、更新サーバは、機器認証クライアントを更新するサービスを提供するサーバ装置であり、更新サーバと、機器認証サーバは、製品コード（製品の機種を特定するコード）と固有鍵生成子との対応関係を同期させて保持しているものとする。

また、対象機器は、更新の対象となる機器認証クライアントを備えた端末機器である。

【０１０４】

まず、対象機器が更新サーバにアクセスし、モジュール（機器認証クライアントに組み込まれた機器認証部９９）の更新を要求する（ステップ４００）。

これに対し、更新サーバは対象機器の機器認証を要求する（ステップ４１０）。

対象機器は、機器認証サーバにアクセスし、機器認証サーバが機器認証を行う（ステップ４０２、ステップ４２２）。

この際に、機器認証サーバは、ワンタイムＩＤを発行して、対象機器の製品コードと対応付けて記憶すると共に、このワンタイムＩＤを対象機器に送信する。

【０１０５】

対象機器は、機器認証サーバからワンタイムＩＤを受信して、これを更新サーバに送信する（ステップ４０４）。

更新サーバは、対象機器からワンタイムＩＤを受信し、これを機器認証サーバに送信する（ステップ４１２）。

機器認証サーバは、更新サーバからワンタイムＩＤを受信し、これに対応付けておいた製品コードを更新サーバに送信する（ステップ４２４）。

【０１０６】

更新サーバは、機器認証サーバから製品コードを受信して、更新対象となっている機器認証クライアントを特定する。

そして、対象機器と通信し、対象機器側の機器認証クライアントのバージョンと最新バージョンの比較などを行いダウンロードするモジュールを確認する（ステップ４０６、ステップ４１４）。

【０１０７】
次に、更新サーバは、製品コードに対応した固有鍵生成子を検索し（ステップ４１６）、この固有鍵生成子に対応したモジュールを生成する（ステップ４１８）。
この際に、モジュールに含まれる公開鍵は、最新のものとなっている。
そして、更新サーバは、生成したモジュールを対象機器にダウンロードする（ステップ４２０）。
対象機器は、ダウンロードしたモジュールを保存する（ステップ４０８）。
【０１０８】
以上のように、本実施の形態では、モジュールを更新することにより、モジュールに含まれる公開鍵を更新するができる。
【０１０９】
[第４の実施の形態]
第１の実施の形態では、ＣＥ機器９は第２のハッシュ値を出力して管理サーバ７に送信し、管理サーバ７がこれを確認したが、本実施の形態では、ＣＥ機器９は、第１のハッシュ値の確認結果を管理サーバ７に送信する。
図１６は、本実施の形態の機器認証部９９ａの構成の一例を示した図である。第１の実施の形態と同じ構成要素には同じ番号を付し、説明を省略する。
機器認証部９９ａは、第１のハッシュ値の確認結果を管理サーバ７に送信する認証情報書込確認モジュール３６を備える。
また、書込モジュール３０ａは、管理サーバ７に第２のハッシュ値を送信する必要がないため、サーバ側確認ハッシュ関数３５（図３）を備えていない。
【０１１０】
書込モジュール３０ａは、管理センタ３から送信されてきた第１のハッシュ値と、機器側確認ハッシュ関数３４による第１のハッシュ値を比較し、その比較結果を認証情報書込確認モジュール３６に出力する。
認証情報書込確認モジュール３６は、更に機器ＩＤを取得し、確認結果と共に接続手段１０を経由して工場システムに出力する。
工場システムは、これに更にシリアル番号を付加して管理サーバ７に送信し、管理センタ３は、確認結果を受け取ることにより、ＣＥ機器９に機器認証情報が組み込まれたことを確認することができる。
【０１１１】
図１７は、本実施の形態において、ＣＥ機器に機器認証情報が適切に組み込まれたことを確認する手順を説明するためのフローチャートである。
図６のフローチャートと同じ処理には同じステップ番号を付し、説明を省略又は簡略化する。
ステップ９０～ステップ１０６までは第１の実施の形態と同じである。
【０１１２】
ただし、ステップ１０６においては、書込モジュール３０ａは、機器側確認ハッシュ関数３４を用いて生成した第１のハッシュ値と管理サーバ７から受信した第１のハッシュ値が同一であるか否かを比較し、その比較結果を認証情報書込確認モジュール３６に出力する（ステップ１０６）。
【０１１３】
認証情報書込確認モジュール３６は、書込モジュール３０ａから比較結果を取得し、また、認証モジュール２０を経由するなどして機器ＩＤ４１を取得し、これらを接続手段１０を経由して工場システムに出力する（ステップ５０２）。
工場システムは、認証情報書込確認モジュール３６から出力された比較結果、及び機器ＩＤに製品シリアル番号を付加し、管理サーバ７に送信する（ステップ５０４）。
【０１１４】
管理サーバ７は、工場システムからこれらの情報を受信する。そして、比較結果により管理サーバ７が送信した第１のハッシュ値と機器側確認ハッシュ関数３４を用いて生成さ

れた第１のハッシュ値が同一であることを確認し、これによって、機器認証情報がＣＥ機器９に記憶されたことを認識する（ステップ５０６）。

【０１１５】

後のステップは第１の実施の形態と同様であり、管理サーバ７は、機器ＩＤと製品シリアル番号を紐付けて記憶し（ステップ１３４）、更に受信したデータに日時情報を付加して秘密鍵で署名し、工場システムに送信する（ステップ１３６）。

工場システムは、署名を確認し、機器認証情報がＣＥ機器９に適切に組み込まれたことを確認する。

【０１１６】

以上のように、本実施の形態では、管理サーバ７は確認結果により、機器認証情報がＣＥ機器９に組み込まれたことを確認することができる。

また、管理サーバ７で第２のハッシュ値を生成する必要がないので管理サーバ７の負荷を低減することができる。

なお、本実施の形態では、書込モジュール３０ａで第１のハッシュ値を生成することとしたが、機器側確認ハッシュ関数３４を認証モジュールに備え、認証モジュールでハッシュ値を生成するように構成してもよい。この場合、認証情報書込確認モジュール３６は、認証モジュールから第１のハッシュ値と機器ＩＤを受け取り、第１のハッシュ値の同一性を確認するように構成できる。

更に、認証情報書込確認モジュール３６の機能を書込モジュール３０ａに持たせ、書込モジュール３０ａが管理サーバ７に確認結果を送信するように構成することもできる。

【図面の簡単な説明】

【０１１７】

【図１】第１の実施の形態の概要を説明するための図である。

【図２】第１の実施の形態における製造認証システムの構成の一例を示した図である。

【図３】第１の実施の形態における機器認証部の構成の一例を示した図である。

【図４】第１の実施の形態において、機器認証情報を組み込む準備段階での作業手順を説明するためのフローチャートである。

【図５】第１の実施の形態において、ＣＥ機器に機器認証情報を組み込む手順を説明するためのフローチャートである。

【図６】第１の実施の形態において、ＣＥ機器に機器認証情報が適切に組み込まれたことを確認する手順を説明するためのフローチャートである。

【図７】第１の実施の形態において、機器認証サーバがＣＥ機器を機器認証する手順を説明するためのフローチャートである。

【図８】第１の実施の形態の機器認証サーバなどに記憶されている各テーブルを説明するための図である。

【図９】第１の実施の形態のＣＥ機器のハードウェア的な構成の一例を示した図である。

【図１０】第２の実施の形態の概要を説明するための図である。

【図１１】第２の実施の形態において、ＣＥ機器に機器認証情報を組み込む手順を説明するためのフローチャートである。

【図１２】第２の実施の形態において、ＣＥ機器に機器認証情報が適切に組み込まれたことを確認する手順を説明するためのフローチャートである。

【図１３】第２の実施の形態において、機器認証サーバがＣＥ機器を機器認証する手順を説明するためのフローチャートである。

【図１４】第２の実施の形態の機器認証サーバなどに記憶されている各テーブルを説明するための図である。

【図１５】第３の実施の形態において、鍵情報が含まれているアプリケーションを更新する手順を説明するためのフローチャートである。

【図１６】第４の実施の形態における機器認証部の構成の一例を示した図である。

【図１７】第４の実施の形態において、ＣＥ機器に機器認証情報が適切に組み込まれたことを確認する手順を説明するためのフローチャートである。

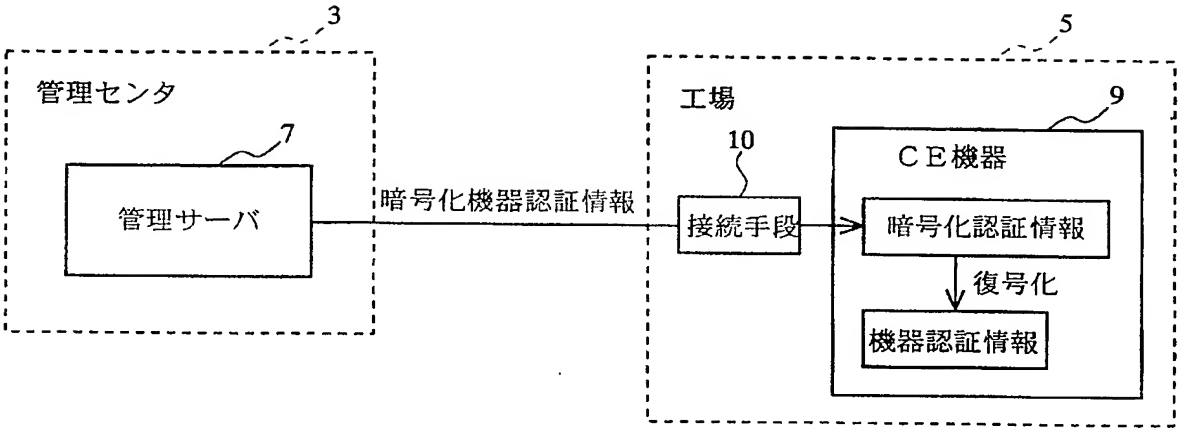
【図１８】従来の認証情報の組み込み方法を説明するための図である。

【符号の説明】

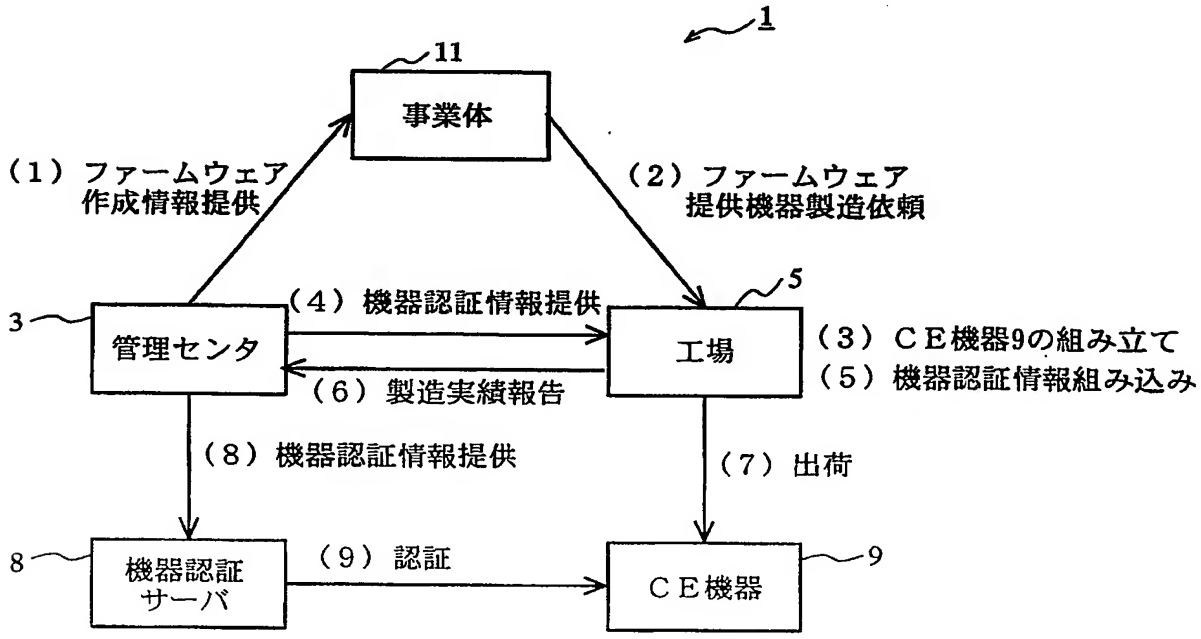
【０１１８】

１	製造認証システム	３	管理センタ
５	工場	７	管理サーバ
８	機器認証サーバ	９	ＣＥ機器
１０	接続手段	１１	事業体
２０	認証モジュール	２１	公開鍵
２２	固有鍵生成子	２３	固有鍵
３０	書込モジュール	３１	書込前鍵
３２	固有鍵生成子	３３	固有鍵
３４	機器側確認ハッシュ関数	３５	サーバ側確認ハッシュ関数
４０	認証情報メモリ	４１	機器ＩＤ
４２	暗号化（機器ＩＤ＋パスフレーズ）	５０	本体識別メモリ
５１	ＭＡＣアドレス	９９	機器認証部

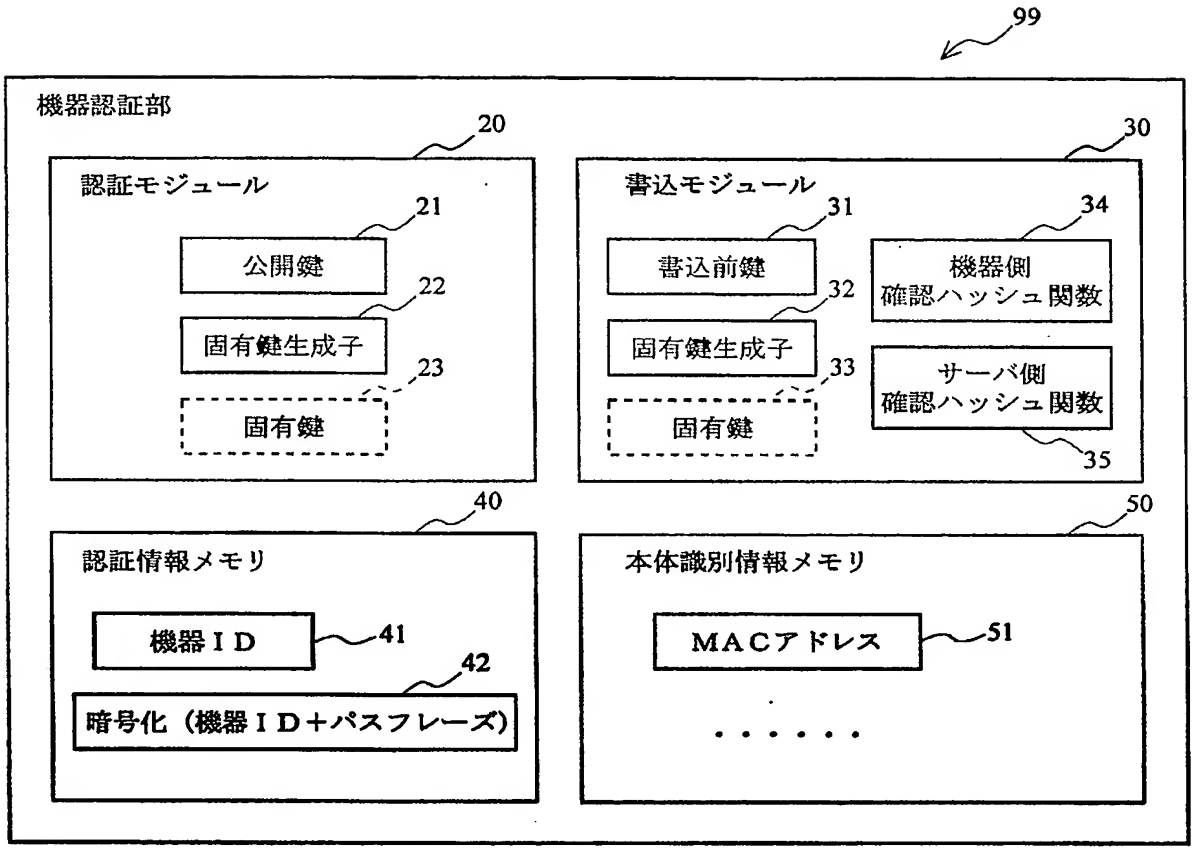
【書類名】図面
【図１】


3
管理センタ
7
管理サーバ
暗号化機器認証情報
5
工場
10
接続手段
9
ＣＥ機器
暗号化認証情報
復号化
機器認証情報

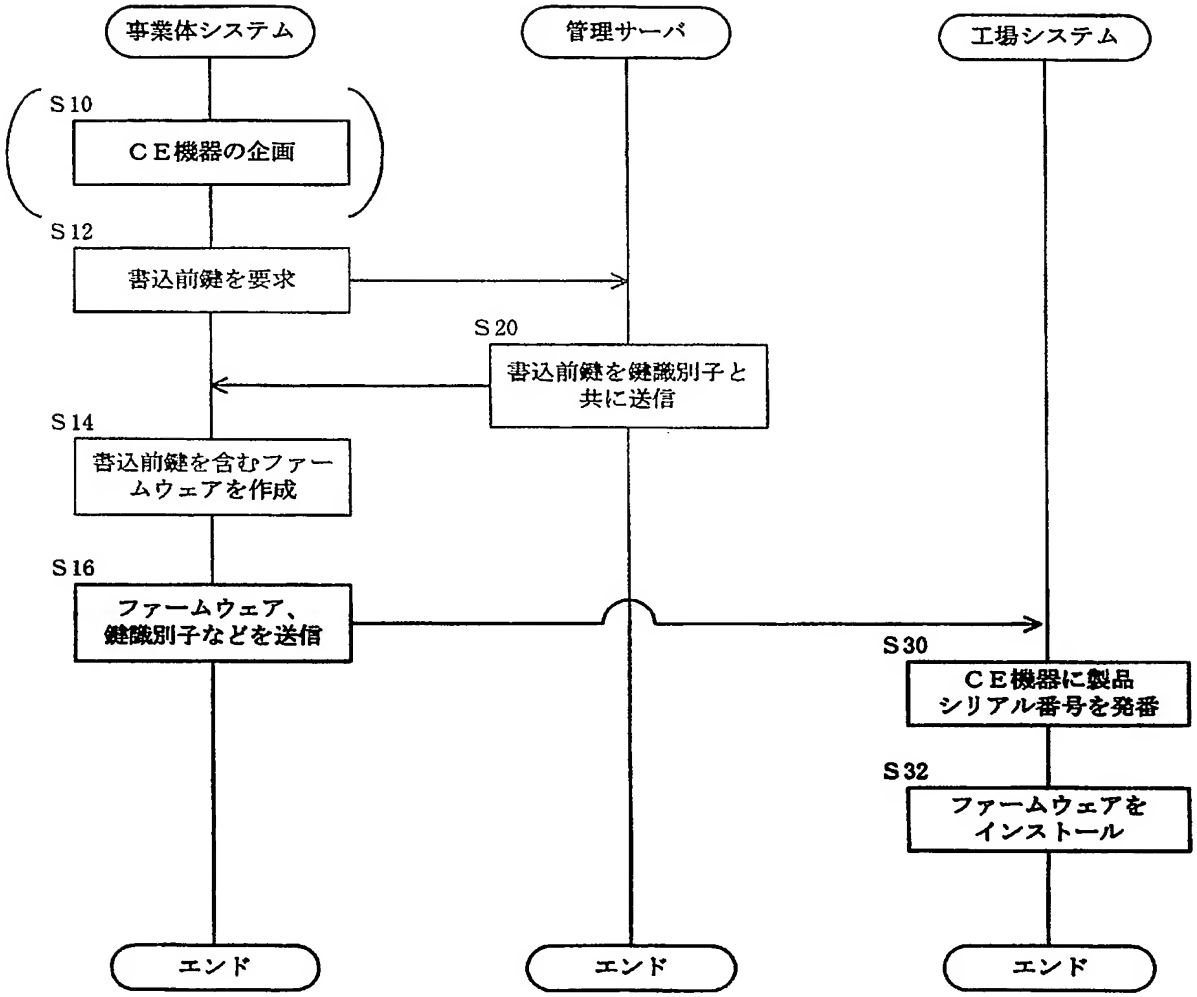
【図２】


1
11
事業体
（1）ファームウェア
作成情報提供
（2）ファームウェア
提供機器製造依頼
3
管理センタ
（4）機器認証情報提供
（6）製造実績報告
5
工場
（3）ＣＥ機器9の組み立て
（5）機器認証情報組み込み
（8）機器認証情報提供
（7）出荷
8
機器認証
サーバ
（9）認証
ＣＥ機器
9

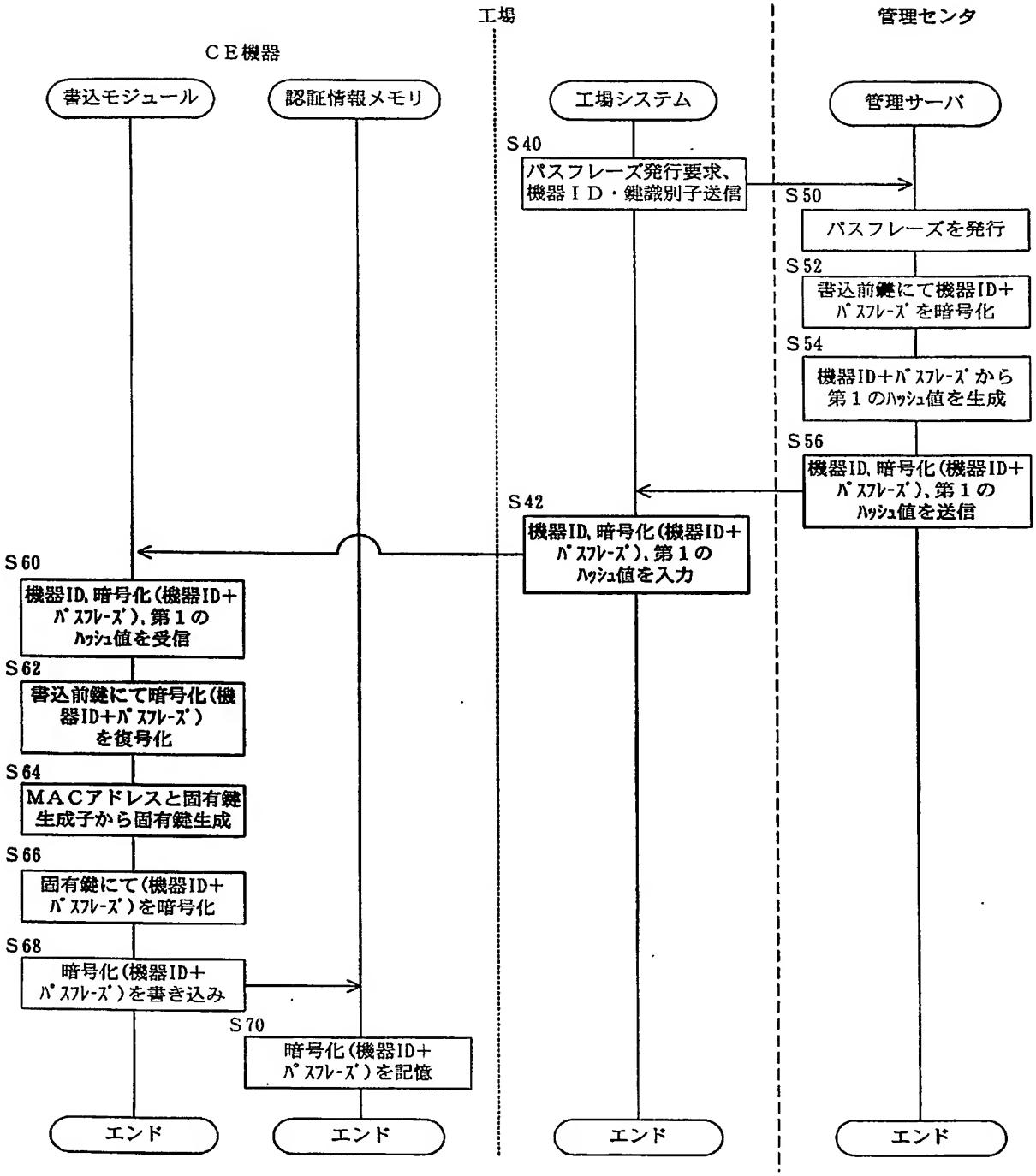
【図３】


99
機器認証部
20
認証モジュール
21
公開鍵
22
固有鍵生成子
23
固有鍵
30
書込モジュール
31
書込前鍵
32
固有鍵生成子
33
固有鍵
34
機器側
確認ハッシュ関数
サーバ側
確認ハッシュ関数
35
40
認証情報メモリ
機器ＩＤ
41
42
暗号化（機器ＩＤ＋パスフレーズ）
50
本体識別情報メモリ
MACアドレス
51
・・・・・・

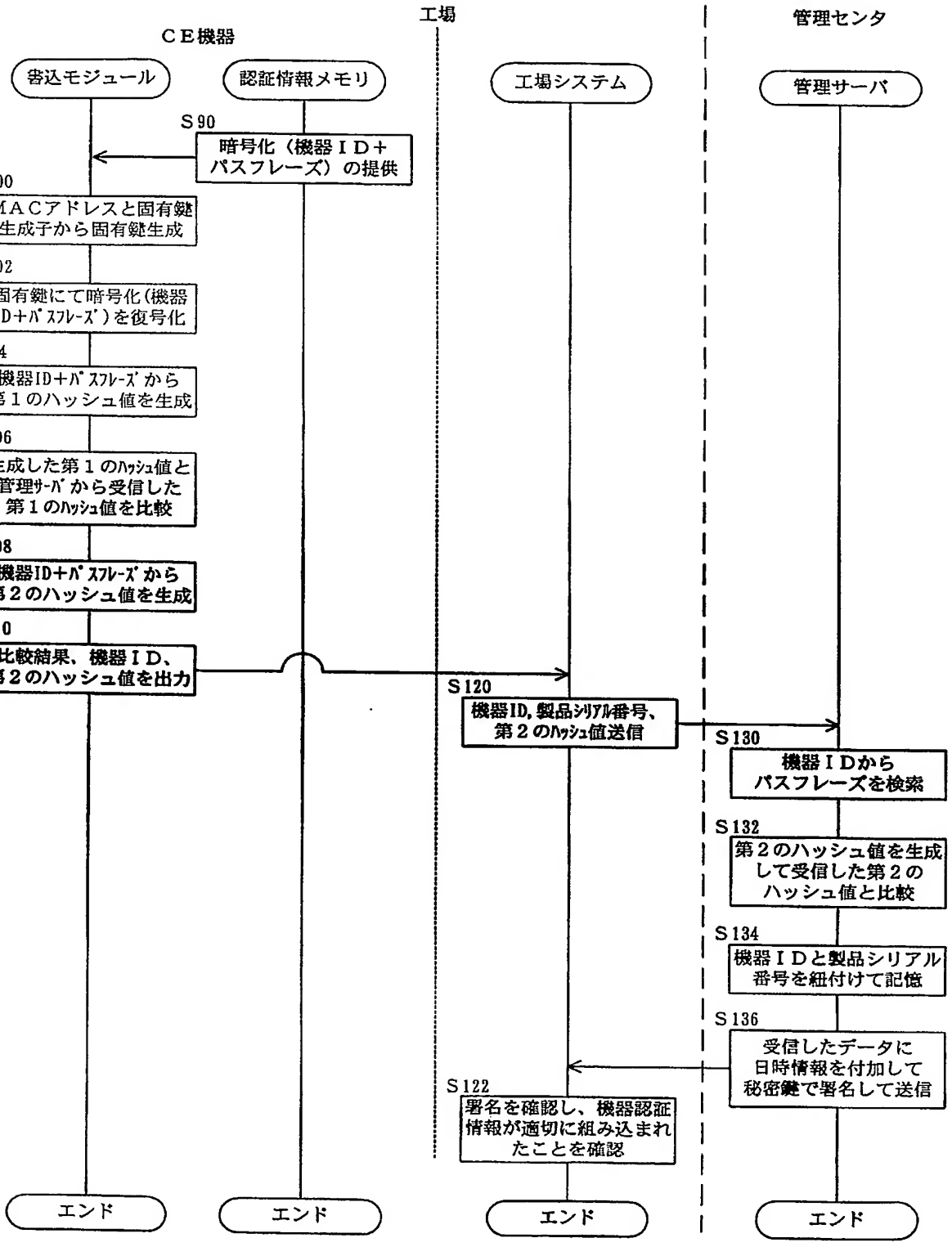
【図４】


事業体システム
管理サーバ
工場システム
S10
ＣＥ機器の企画
S12
書込前鍵を要求
S20
書込前鍵を鍵識別子と共に送信
S14
書込前鍵を含むファームウェアを作成
S16
ファームウェア、鍵識別子などを送信
S30
ＣＥ機器に製品シリアル番号を発番
S32
ファームウェアをインストール
エンド
エンド
エンド

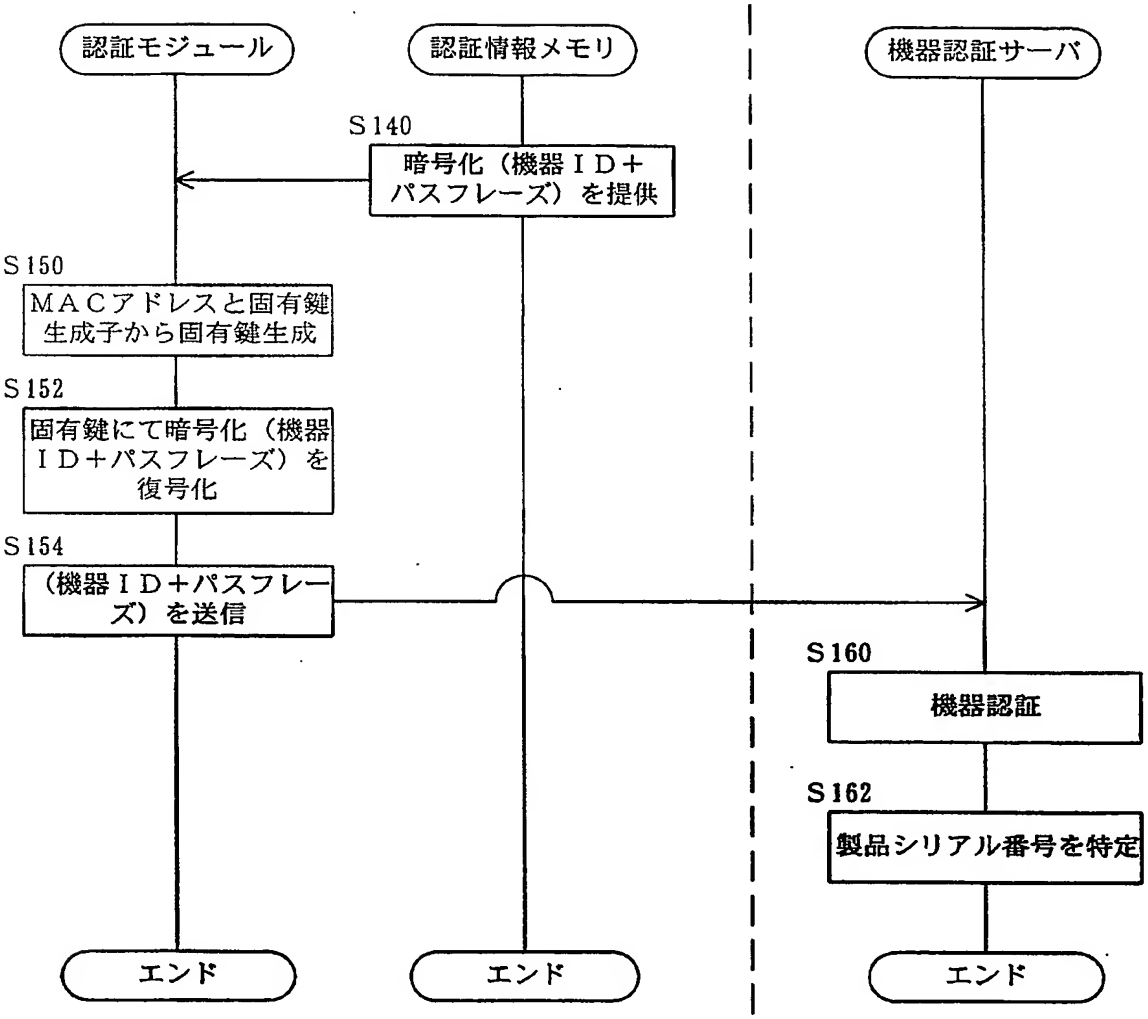
【図５】


工場
管理センタ
ＣＥ機器
書込モジュール
認証情報メモリ
工場システム
管理サーバ
S40
パスフレーズ発行要求、機器ＩＤ・鍵識別子送信
S50
パスフレーズを発行
S52
書込前鍵にて機器ID+ﾊﾟｽﾌﾚｰｽﾞを暗号化
S54
機器ID+ﾊﾟｽﾌﾚｰｽﾞから第１のﾊｯｼｭ値を生成
S56
機器ID、暗号化（機器ID+ﾊﾟｽﾌﾚｰｽﾞ）、第１のﾊｯｼｭ値を送信
S42
機器ID、暗号化（機器ID+ﾊﾟｽﾌﾚｰｽﾞ）、第１のﾊｯｼｭ値を入力
S60
機器ID、暗号化（機器ID+ﾊﾟｽﾌﾚｰｽﾞ）、第１のﾊｯｼｭ値を受信
S62
書込前鍵にて暗号化（機器ID+ﾊﾟｽﾌﾚｰｽﾞ）を復号化
S64
ＭＡＣアドレスと固有鍵生成子から固有鍵生成
S66
固有鍵にて（機器ID+ﾊﾟｽﾌﾚｰｽﾞ）を暗号化
S68
暗号化（機器ID+ﾊﾟｽﾌﾚｰｽﾞ）を書き込み
S70
暗号化（機器ID+ﾊﾟｽﾌﾚｰｽﾞ）を記憶
エンド
エンド
エンド
エンド

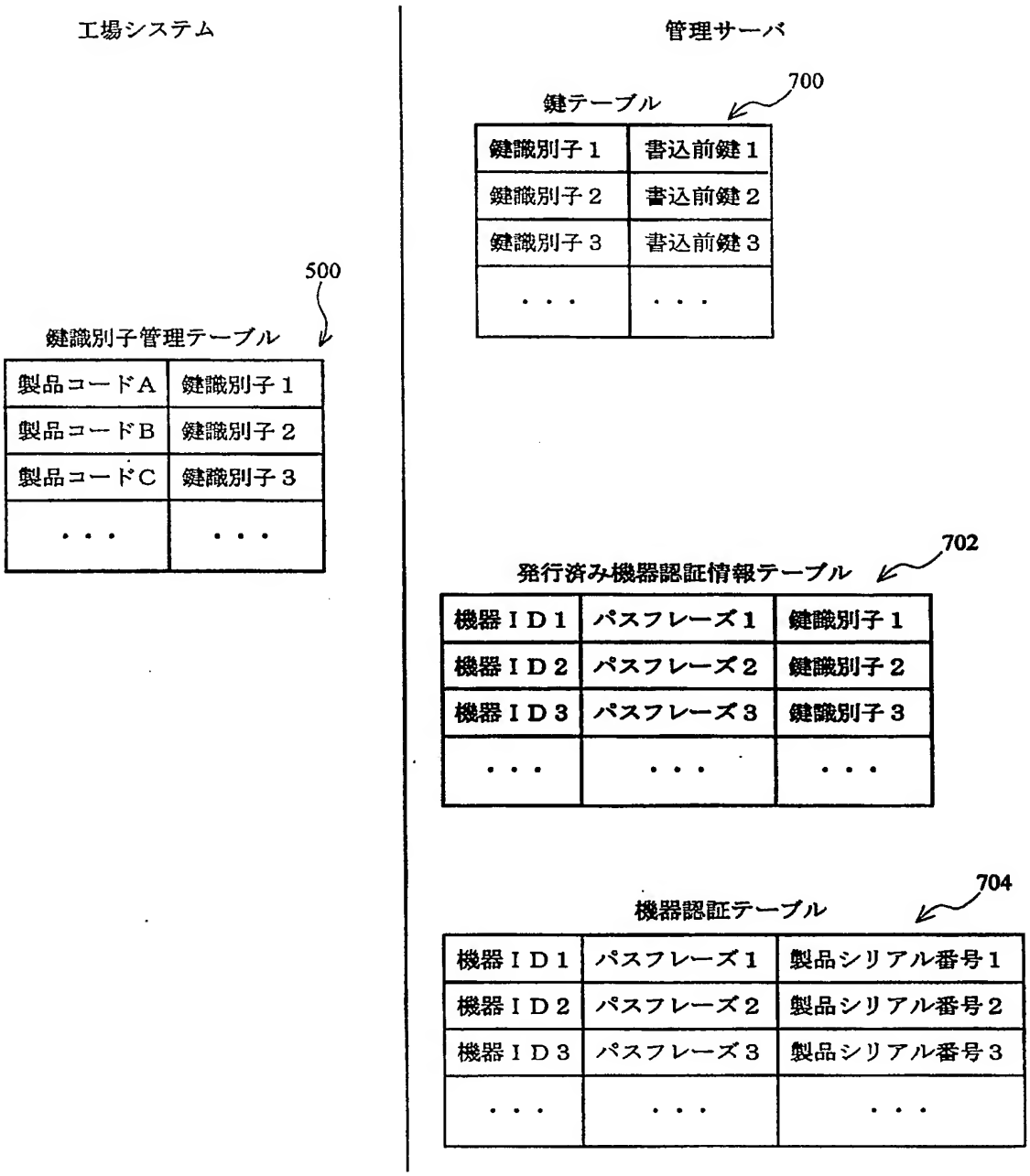
【図６】


CE機器
工場
管理センタ
害込モジュール
認証情報メモリ
工場システム
管理サーバ
S90
暗号化（機器ＩＤ＋パスフレーズ）の提供
S100
MACアドレスと固有鍵生成子から固有鍵生成
S102
固有鍵にて暗号化(機器ID+ﾊﾟｽﾌﾚｰｽﾞ)を復号化
S104
機器ID+ﾊﾟｽﾌﾚｰｽﾞから第１のハッシュ値を生成
S106
生成した第１のﾊｯｼｭ値と管理ｻｰﾊﾞから受信した第１のﾊｯｼｭ値を比較
S108
機器ID+ﾊﾟｽﾌﾚｰｽﾞから第２のハッシュ値を生成
S110
比較結果、機器ＩＤ、第２のハッシュ値を出力
S120
機器ID,製品ｼﾘｱﾙ番号、第２のﾊｯｼｭ値送信
S130
機器ＩＤからパスフレーズを検索
S132
第２のハッシュ値を生成して受信した第２のハッシュ値と比較
S134
機器ＩＤと製品シリアル番号を紐付けて記憶
S136
受信したデータに日時情報を付加して秘密鍵で署名して送信
S122
署名を確認し、機器認証情報が適切に組み込まれたことを確認
エンド
エンド
エンド
エンド

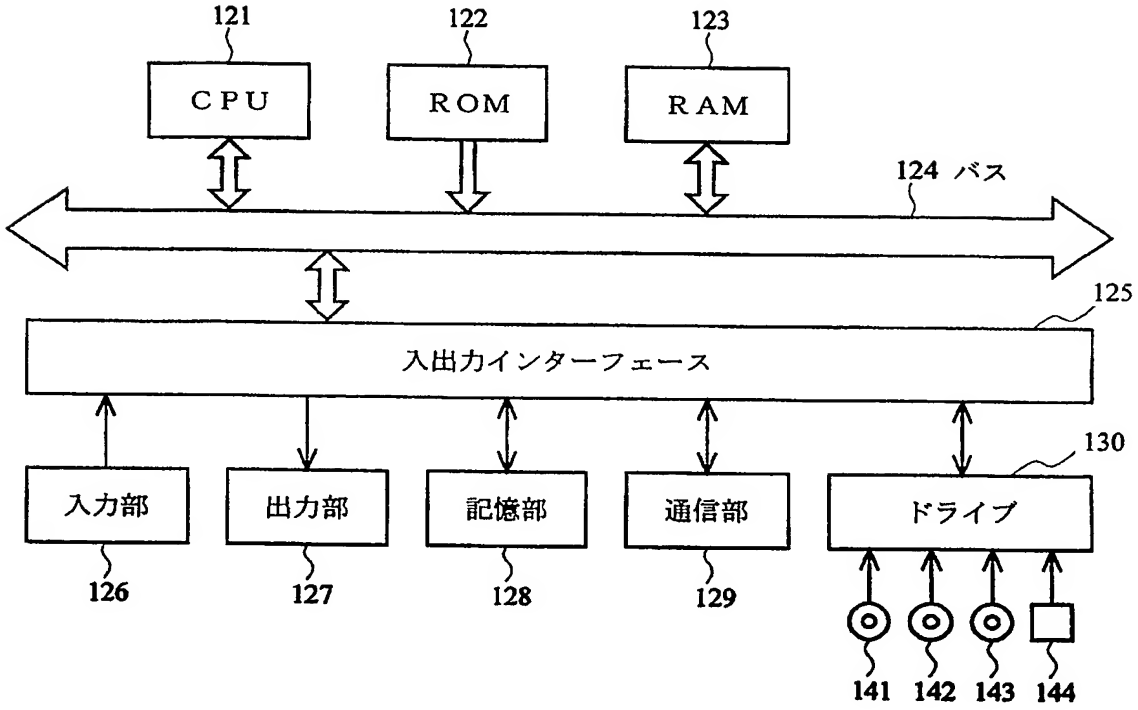
【図７】


認証モジュール
認証情報メモリ
機器認証サーバ
S140
暗号化（機器ＩＤ＋パスフレーズ）を提供
S150
ＭＡＣアドレスと固有鍵生成子から固有鍵生成
S152
固有鍵にて暗号化（機器ＩＤ＋パスフレーズ）を復号化
S154
（機器ＩＤ＋パスフレーズ）を送信
S160
機器認証
S162
製品シリアル番号を特定
エンド
エンド
エンド

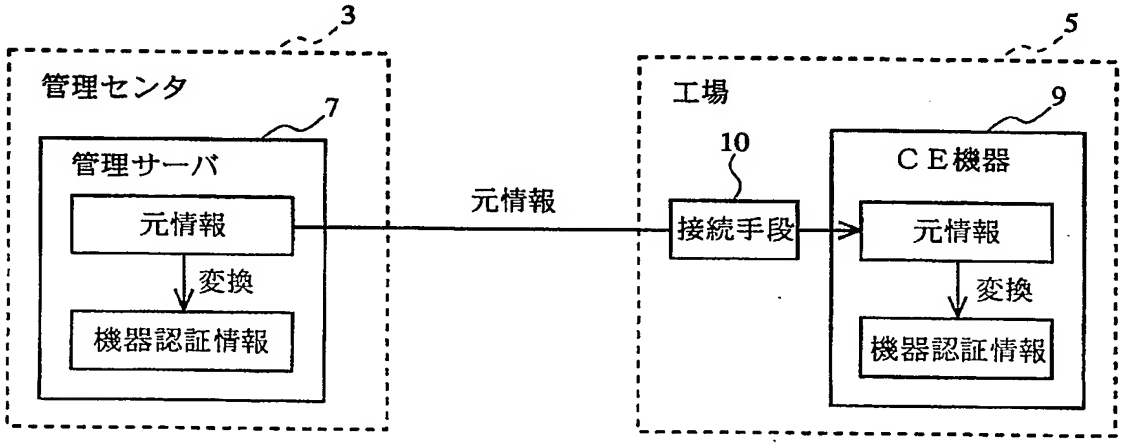
【図８】


工場システム
管理サーバ
700
鍵テーブル
鍵識別子１
書込前鍵１
鍵識別子２
書込前鍵２
鍵識別子３
書込前鍵３
500
鍵識別子管理テーブル
製品コードＡ
鍵識別子１
製品コードＢ
鍵識別子２
製品コードＣ
鍵識別子３
702
発行済み機器認証情報テーブル
機器ＩＤ１
パスフレーズ１
鍵識別子１
機器ＩＤ２
パスフレーズ２
鍵識別子２
機器ＩＤ３
パスフレーズ３
鍵識別子３
704
機器認証テーブル
機器ＩＤ１
パスフレーズ１
製品シリアル番号１
機器ＩＤ２
パスフレーズ２
製品シリアル番号２
機器ＩＤ３
パスフレーズ３
製品シリアル番号３

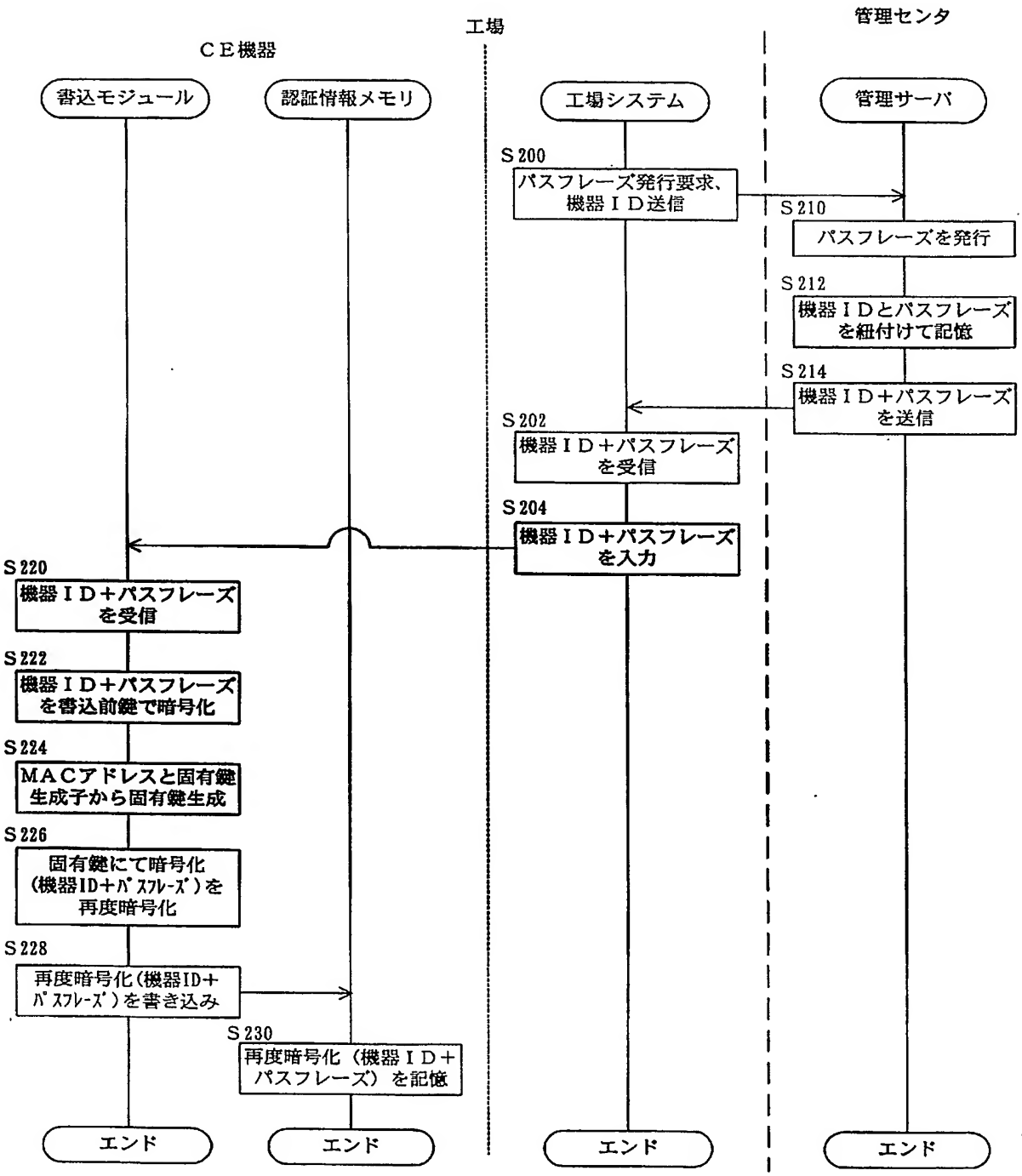
【図９】


121
CPU
122
ROM
123
RAM
124 バス
125
入出力インターフェース
130
入力部
出力部
記憶部
通信部
ドライブ
126
127
128
129
141
142
143
144

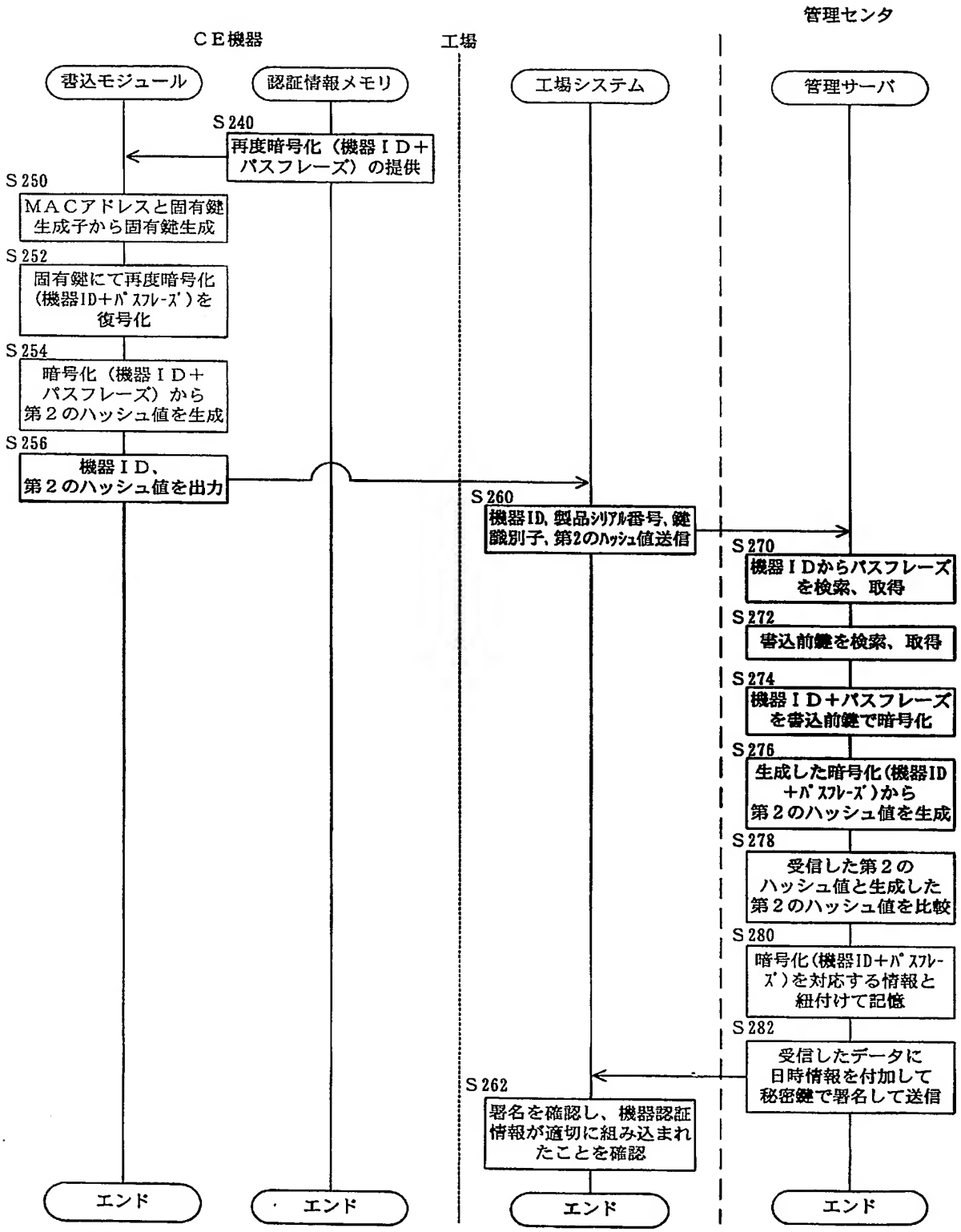
【図１０】


3
管理センタ
7
管理サーバ
元情報
変換
機器認証情報
元情報
5
工場
10
接続手段
9
ＣＥ機器
元情報
変換
機器認証情報

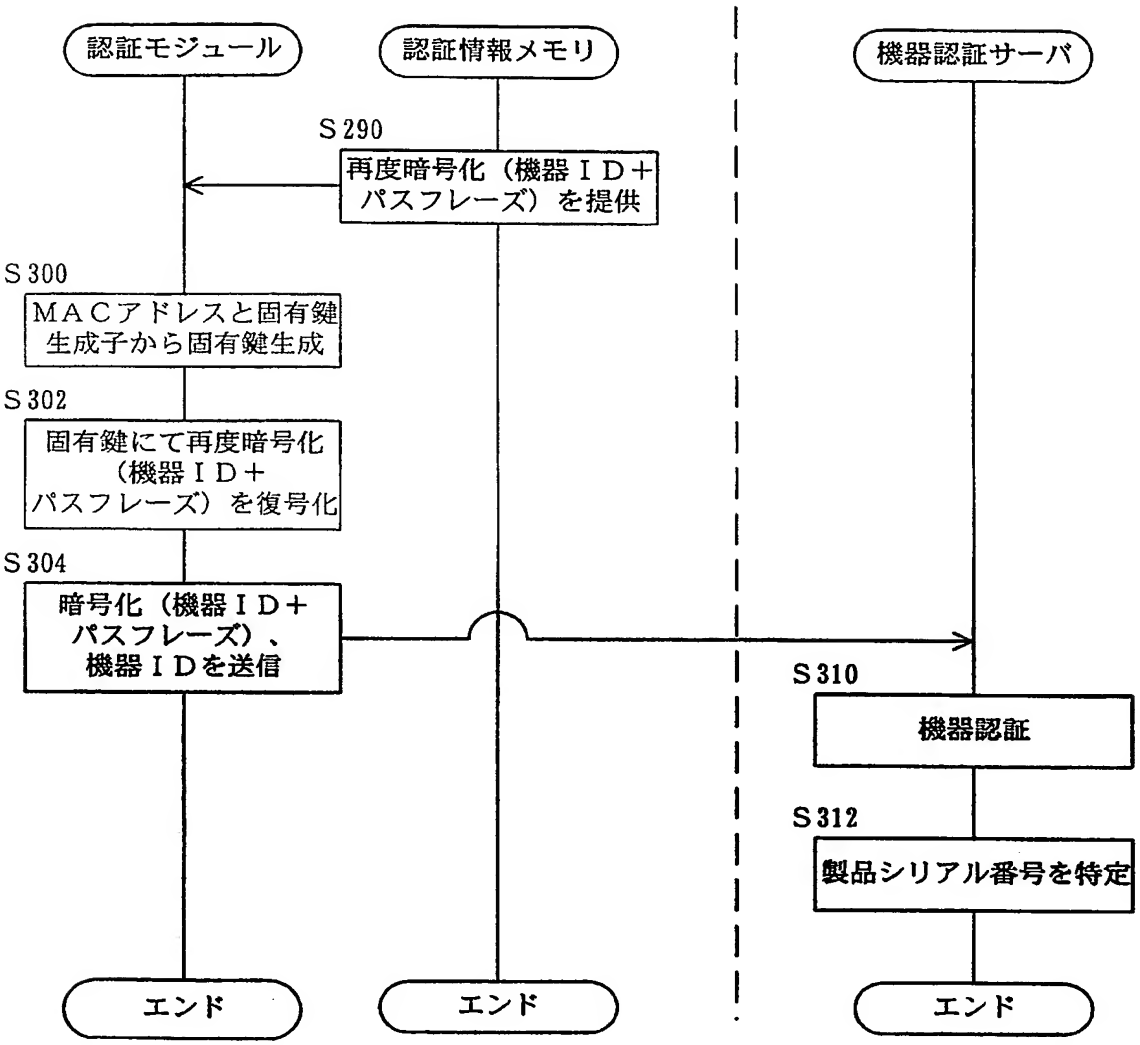
【図１１】


工場
管理センタ
ＣＥ機器
書込モジュール
認証情報メモリ
工場システム
管理サーバ
S200
パスフレーズ発行要求、機器ＩＤ送信
S210
パスフレーズを発行
S212
機器ＩＤとパスフレーズを紐付けて記憶
S214
機器ＩＤ＋パスフレーズを送信
S202
機器ＩＤ＋パスフレーズを受信
S204
機器ＩＤ＋パスフレーズを入力
S220
機器ＩＤ＋パスフレーズを受信
S222
機器ＩＤ＋パスフレーズを書込前鍵で暗号化
S224
ＭＡＣアドレスと固有鍵生成子から固有鍵生成
S226
固有鍵にて暗号化（機器ID＋ﾊﾟｽﾌﾚｰｽﾞ）を再度暗号化
S228
再度暗号化（機器ID＋ﾊﾟｽﾌﾚｰｽﾞ）を書き込み
S230
再度暗号化（機器ＩＤ＋パスフレーズ）を記憶
エンド
エンド
エンド
エンド

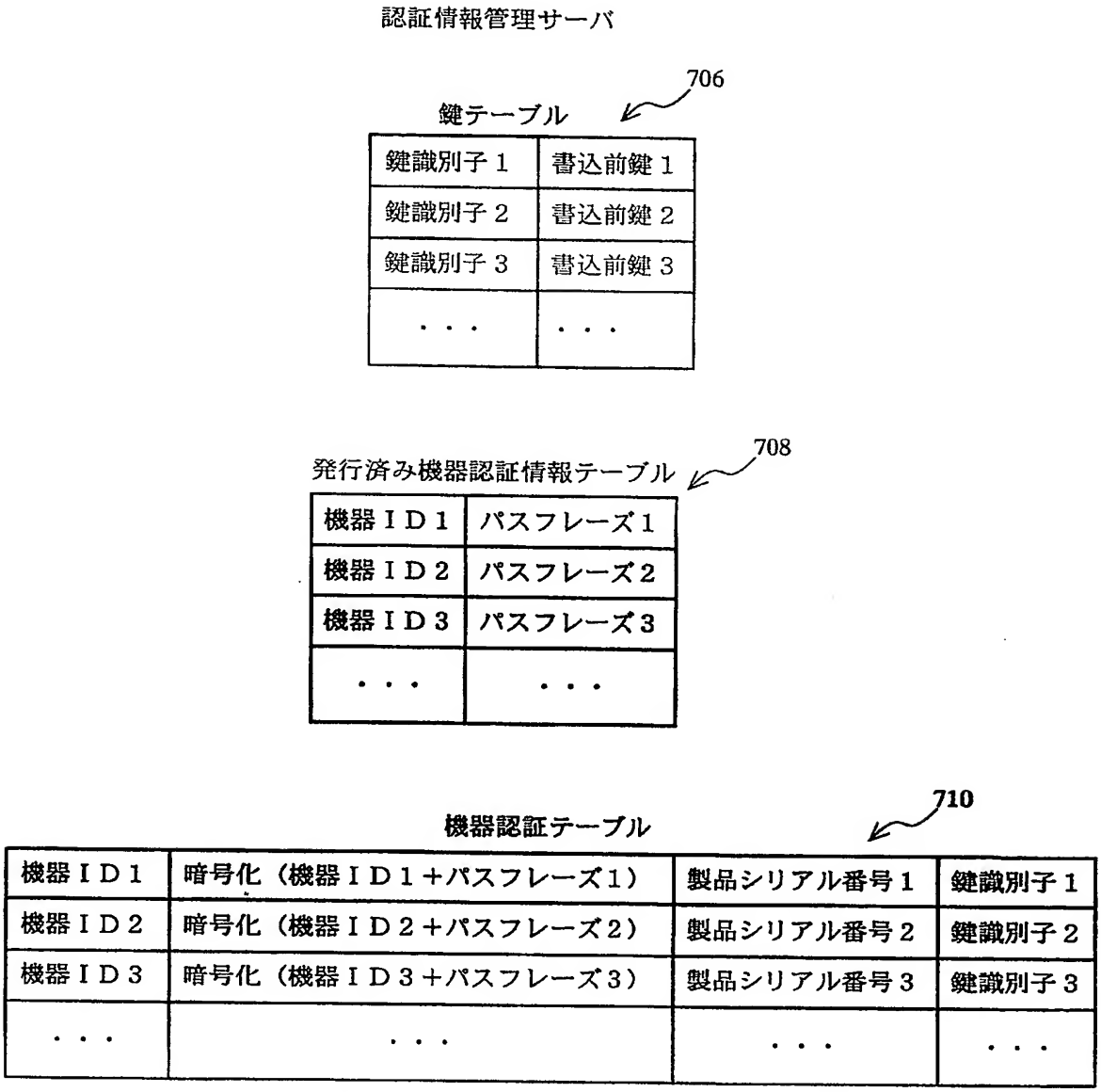
【図１２】


ＣＥ機器
工場
管理センタ
書込モジュール
認証情報メモリ
工場システム
管理サーバ
S240
再度暗号化（機器ＩＤ＋パスフレーズ）の提供
S250
ＭＡＣアドレスと固有鍵生成子から固有鍵生成
S252
固有鍵にて再度暗号化（機器ID＋ﾊﾟｽﾌﾚｰｽﾞ）を復号化
S254
暗号化（機器ＩＤ＋パスフレーズ）から第２のハッシュ値を生成
S256
機器ＩＤ、第２のハッシュ値を出力
S260
機器ID, 製品ｼﾘｱﾙ番号, 鍵識別子, 第2のﾊｯｼｭ値送信
S270
機器ＩＤからパスフレーズを検索、取得
S272
書込前鍵を検索、取得
S274
機器ＩＤ＋パスフレーズを書込前鍵で暗号化
S276
生成した暗号化（機器ID＋ﾊﾟｽﾌﾚｰｽﾞ）から第２のハッシュ値を生成
S278
受信した第２のハッシュ値と生成した第２のハッシュ値を比較
S280
暗号化（機器ID＋ﾊﾟｽﾌﾚｰｽﾞ）を対応する情報と紐付けて記憶
S282
受信したデータに日時情報を付加して秘密鍵で署名して送信
S262
署名を確認し、機器認証情報が適切に組み込まれたことを確認
エンド
エンド
エンド
エンド

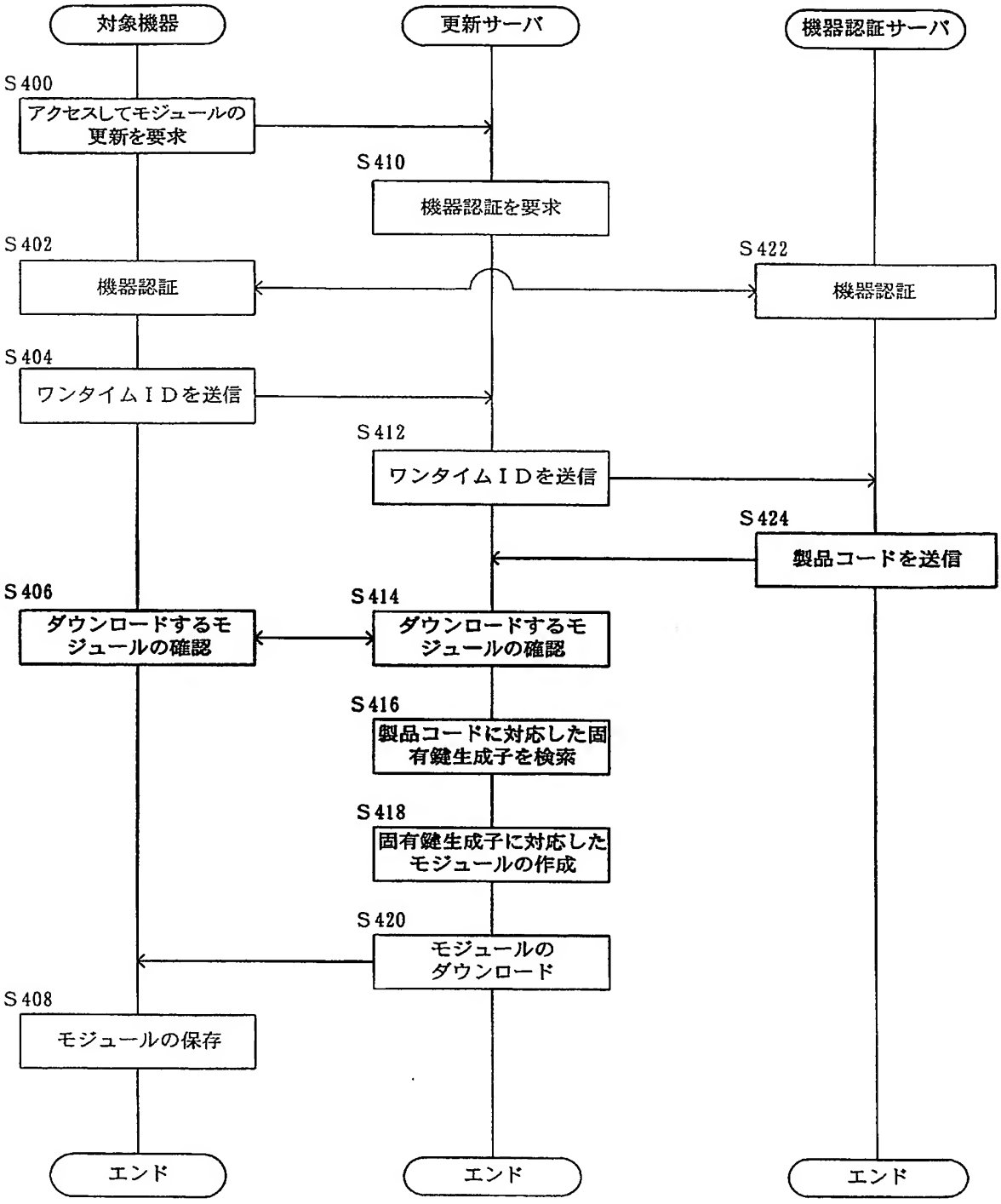
【図１３】


認証モジュール
認証情報メモリ
機器認証サーバ
S290
再度暗号化（機器ＩＤ＋パスフレーズ）を提供
S300
ＭＡＣアドレスと固有鍵生成子から固有鍵生成
S302
固有鍵にて再度暗号化（機器ＩＤ＋パスフレーズ）を復号化
S304
暗号化（機器ＩＤ＋パスフレーズ）、機器ＩＤを送信
S310
機器認証
S312
製品シリアル番号を特定
エンド
エンド
エンド

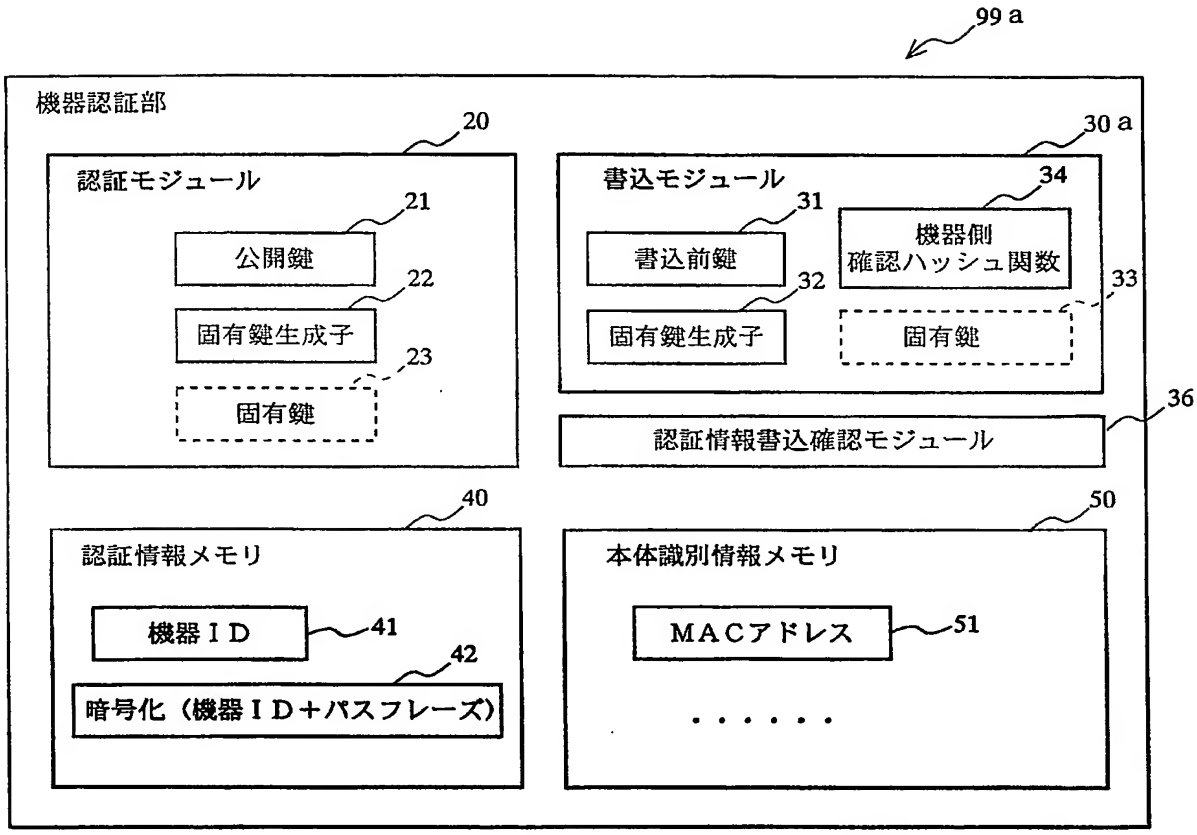
【図１４】


認証情報管理サーバ
706
鍵テーブル
鍵識別子１
書込前鍵１
鍵識別子２
書込前鍵２
鍵識別子３
書込前鍵３
・・・
・・・
708
発行済み機器認証情報テーブル
機器ＩＤ１
パスフレーズ１
機器ＩＤ２
パスフレーズ２
機器ＩＤ３
パスフレーズ３
・・・
・・・
710
機器認証テーブル
機器ＩＤ１
暗号化（機器ＩＤ１＋パスフレーズ１）
製品シリアル番号１
鍵識別子１
機器ＩＤ２
暗号化（機器ＩＤ２＋パスフレーズ２）
製品シリアル番号２
鍵識別子２
機器ＩＤ３
暗号化（機器ＩＤ３＋パスフレーズ３）
製品シリアル番号３
鍵識別子３
・・・
・・・
・・・
・・・

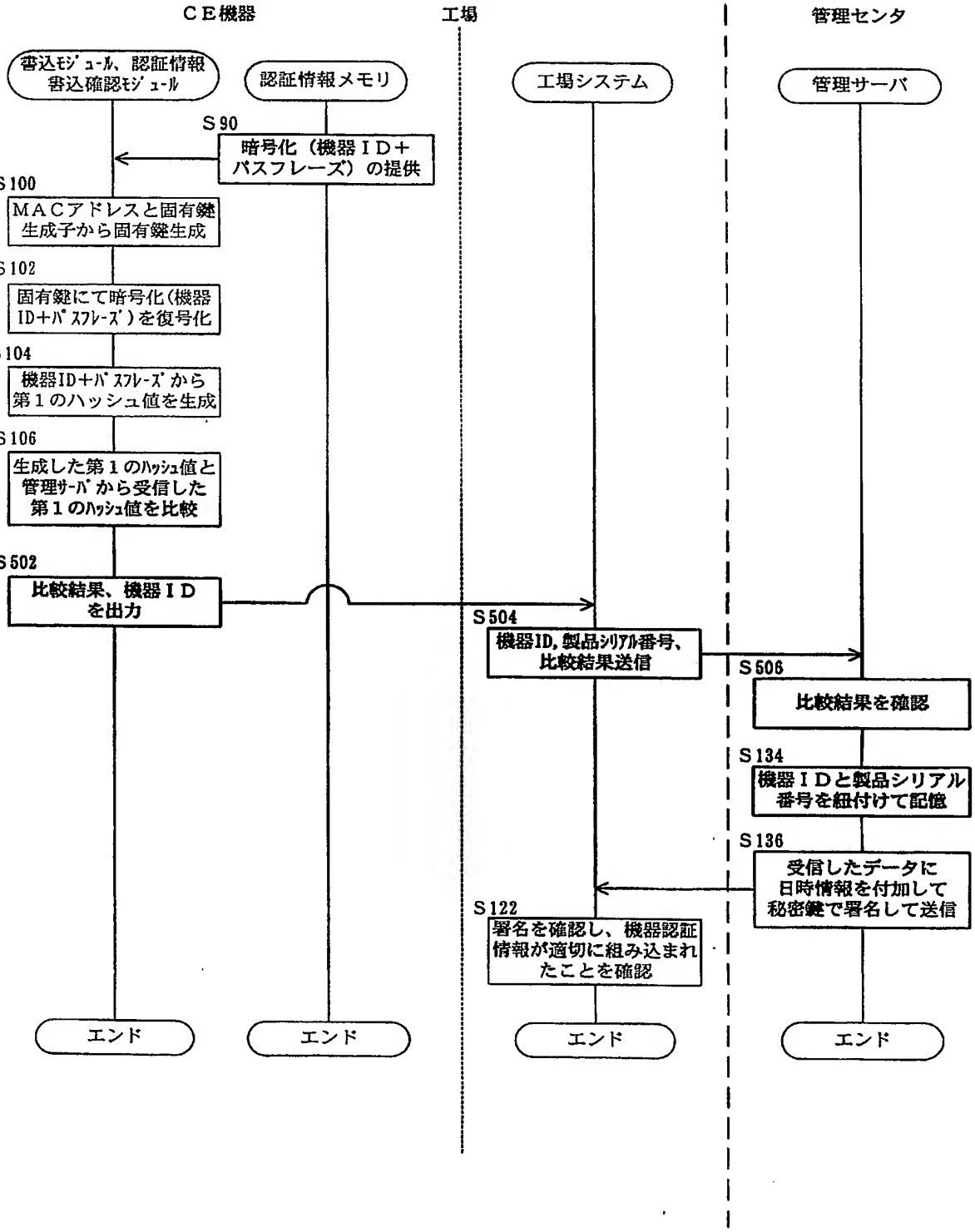
【図１５】


対象機器
更新サーバ
機器認証サーバ
S400
アクセスしてモジュールの更新を要求
S410
機器認証を要求
S402
機器認証
S422
機器認証
S404
ワンタイムＩＤを送信
S412
ワンタイムＩＤを送信
S424
製品コードを送信
S406
ダウンロードするモジュールの確認
S414
ダウンロードするモジュールの確認
S416
製品コードに対応した固有鍵生成子を検索
S418
固有鍵生成子に対応したモジュールの作成
S420
モジュールのダウンロード
S408
モジュールの保存
エンド
エンド
エンド

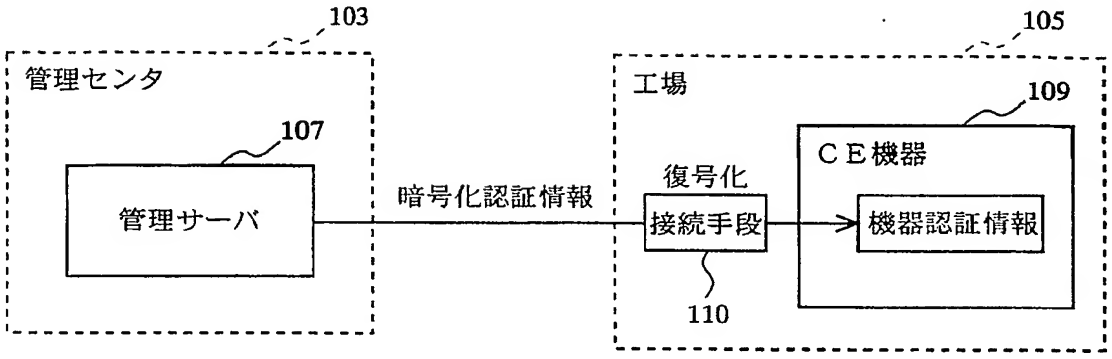
【図１６】


99 a
機器認証部
20
認証モジュール
21
公開鍵
22
固有鍵生成子
23
固有鍵
30 a
書込モジュール
31
書込前鍵
32
固有鍵生成子
34
機器側
確認ハッシュ関数
33
固有鍵
36
認証情報書込確認モジュール
40
認証情報メモリ
機器ＩＤ
41
42
暗号化（機器ＩＤ＋パスフレーズ）
50
本体識別情報メモリ
ＭＡＣアドレス
51
・・・・・・

【図１７】


ＣＥ機器
工場
管理センタ
書込ﾓｼﾞｭｰﾙ、認証情報書込確認ﾓｼﾞｭｰﾙ
認証情報メモリ
工場システム
管理サーバ
S90
暗号化（機器ＩＤ＋パスフレーズ）の提供
S100
ＭＡＣアドレスと固有鍵生成子から固有鍵生成
S102
固有鍵にて暗号化(機器ID+ﾊﾟｽﾌﾚｰｽﾞ)を復号化
S104
機器ID+ﾊﾟｽﾌﾚｰｽﾞから第１のハッシュ値を生成
S106
生成した第１のﾊｯｼｭ値と管理ｻｰﾊﾞから受信した第１のﾊｯｼｭ値を比較
S502
比較結果、機器ＩＤを出力
S504
機器ID,製品ｼﾘｱﾙ番号、比較結果送信
S506
比較結果を確認
S134
機器ＩＤと製品シリアル番号を紐付けて記憶
S136
受信したデータに日時情報を付加して秘密鍵で署名して送信
S122
署名を確認し、機器認証情報が適切に組み込まれたことを確認
エンド
エンド
エンド
エンド

【図１８】


103
管理センタ
107
管理サーバ
暗号化認証情報
105
工場
109
ＣＥ機器
復号化
接続手段
機器認証情報
110

【書類名】要約書
【要約】
【課題】　ＣＥ機器内に機器認証情報を安全に組み込むこと。
【解決手段】　管理サーバ７は、機器認証情報を暗号化して工場５に送信する。接合具１０は、工場の作業者によりＣＥ機器９のコネクタに接続され、管理サーバ７から送信されてきた機器認証情報を暗号化されたままＣＥ機器９に入力する。ＣＥ機器９の内部には、暗号化された機器認証情報を復号化して格納するための書込モジュールが内蔵されている。接合具１０から入力された機器認証情報は、書込モジュールにより復号化され、ＣＥ機器９内部の記憶装置に記憶される。機器認証情報は、暗号化されたままＣＥ機器９に入力されるので安全に機器認証情報を組み込むことができる。
【選択図】　図１

認定・付加情報

特許出願の番号	特願２００４－１７９５６２
受付番号	５０４０１０２０７１７
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１６年　６月２２日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】	000002185
【住所又は居所】	東京都品川区北品川６丁目７番３５号
【氏名又は名称】	ソニー株式会社

【代理人】　申請人

【識別番号】	100096655
【住所又は居所】	東京都新宿区西新宿８－１２－８　梅屋ビルＢ１
【氏名又は名称】	川井　隆

【選任した代理人】

【識別番号】	100091225
【住所又は居所】	東京都新宿区西新宿８－１２－８　梅屋ビルＢ１
【氏名又は名称】	仲野　均

特願２００４－１７９５６２

出　願　人　履　歴　情　報

識別番号　　[０００００２１８５]

１．変更年月日　　１９９０年　８月３０日
[変更理由]　　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☑ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.